AEE

AEE

18CV2120

BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	MDL DOCKET NO. 2843

FACEBOOK, INC.'S RESPONSE IN SUPPORT OF PLAINTIFFS' MOTIONS TO TRANSFER RELATED CASES FOR CONSOLIDATED PRETRIAL PROCEEDINGS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes & Rules

Other Authorities

I. INTRODUCTION

Facebook respectfully submits this response to support the plaintiffs' motions to establish a multidistrict litigation ("MDL") proceeding for consumer class action arising from recent events involving Cambridge Analytica. Facebook agrees with the plaintiffs that organizing these cases into an MDL would create substantial efficiencies and avoid inconsistent rulings. Facebook also agrees with the *Beiner* and *Rubin* plaintiffs that the Northern District of California is the most appropriate transferee district.

In the wake of recent press reports describing the alleged misuse of Facebook user data, fourteen consumer class actions have been filed in six federal districts. Facebook is strongly committed to protecting users' information, and it has already taken and continues to take substantial actions to address the conduct that gave rise to these cases. But the lawsuits that have been filed against Facebook are misguided: Facebook broke no laws and violated no legal duties. And although Cambridge Analytica and other related actors used data for purposes that Facebook and its users never authorized, there was no data breach—no unauthorized access to Facebook's systems and no hacking of user data.

All of the cases seek to certify nationwide classes of Facebook accountholders based on the same alleged underlying facts: that a third-party app developer named Aleksandr Kogan, beginning in 2013, used an app he created to obtain information about Facebook users by paying them to take a personality test in exchange for their agreement that the information could be used for academic purposes; that Kogan collected information about those individuals and their Facebook "friends" and then shared that information, through his company Global Science Research ("GSR"), with Cambridge Analytica, contrary to Facebook's terms of service; that Kogan, GSR, Cambridge Analytica, and others each certified that they had deleted this data in

response to Facebook's demands; and that Cambridge Analytica still apparently used the data to target advertisements in connection with the 2016 U.S. Presidential election. All of the cases are at the earliest stage, having been filed in the last few weeks with no substantive motions filed or scheduling conferences held. All of these putative class actions name Cambridge Analytica and Facebook as defendants, and several also name Kogan and GSR. And while the actions assert a variety of related and overlapping legal theories, all of them suffer from similar deficiencies.

Facebook agrees with plaintiffs that an MDL is the most efficient and sensible way to handle pretrial proceedings in these actions and the copycat actions likely to follow in the coming weeks and months. Should this panel agree to establish an MDL, Facebook agrees with the *Beiner* and *Rubin* plaintiffs that the Northern District of California is the most appropriate venue. Nine of the fourteen consumer class actions have been filed in that district, which also is home to a closely related series of shareholder class actions pending before Judge Edward J. Davila based on the same news reports about Cambridge Analytica. Facebook is headquartered in the district and many relevant witnesses are likely to be located there. And, as this panel is aware, judges in the Northern District of California are well-versed in handing MDL proceedings involving multiple class actions like those at issue here, and there is an ample body of Ninth Circuit precedent on class certification and other relevant issues. In light of these circumstances, the Northern District of California is the most sensible and efficient forum for these putative class actions.

II. BACKGROUND

The litigation pertaining to Cambridge Analytica followed on the heels of two news articles published on March 17, 2018, by *The New York Times* and *The Guardian*.[1] The actions fall into three broad categories: (1) shareholder class actions brought under the federal securities laws, all filed in the Northern District of California;[2] (2) shareholder derivative class actions, also all filed in the Northern District of California;[3] and (3) fourteen consumer class action suits brought under various federal and state law theories, pending in six different districts, including the Northern District of California. Plaintiffs' motions, and this response, relate to the third category—the consumer cases—which includes the following actions (the particulars of which are set out in more detail in Appendices to this brief, as noted below):

a. **Northern District of California**:

i. *Beiner v. Facebook, Inc.*, No. 3:18-CV-1953 (N.D. Cal.) (filed Mar. 29, 2018) (Corley, M.J.)

---

[1] M. Rosenberg, N. Confessore & C. Cadwalladr, *How Trump "Consultants" Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html; C. Cadwalladr & E. Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[2] *Yuan v. Facebook, Inc.*, No. 5:18-CV-01725 (N.D. Cal.) (filed Mar. 20, 2018) (Davila, J.); *Casey v. Facebook, Inc.*, No. 5:18-CV-01780 (N.D. Cal.) (filed Mar. 22, 2018) (Davila, J.); *Ernestine v. Facebook, Inc.*, No. 3:18-CV-01868 (N.D. Cal.) (filed Mar. 27, 2018) (Alsup, J.).

[3] *Hallisey v. Zuckerberg*, 4:18-CV-01792 (N.D. Cal.) (filed Mar. 22, 2018) (pending before Gilliam, J.); *Martin v. Zuckerberg*, No. 4:18-CV-01834 (N.D. Cal.) (filed Mar. 23, 2018) (pending before Ryu, M.J.); *Ocegueda v. Zuckerberg*, No. 4:18-CV-01893 (N.D. Cal.) (filed Mar. 27, 2018) (Westmore, M.J.); *Karon v. Facebook, Inc.*, No. 5:18-CV-01929 (N.D. Cal.) (pending before Cousins, J.); *Gloria Stricklin Trust v. Zuckerberg*, No. 3:18-CV-02011 (N.D. Cal.) (filed Apr. 2, 2018) (pending before Corley, M.J.).

ii. *Gennock v. Facebook, Inc.*, No. 3:18-CV-01891 (N.D. Cal.) (filed Mar. 27, 2018) (Ryu, M.J.)

iii. *Haslinger v. Facebook, Inc.*, No. 3:18-CV-01984 (N.D. Cal.) (filed Mar. 30, 2018) (Rogers, J.)

iv. *Kooser v. Facebook, Inc.*, No. 3:18-cv-02009 (N.D. Cal.) (filed Apr. 2, 2018) (Laporte, M.J.)

v. *Labajo v. Facebook, Inc.*, No. 4:18-CV-02093 (N.D. Cal.) (filed Apr. 5, 2018) (Westmore, M.J.)

vi. *O'Kelly v. Facebook, Inc.*, No. 3:18-CV-01915 (N.D. Cal.) (filed Mar. 28, 2018) (Laporte, M.J.)

vii. *Picha v. Facebook, Inc.*, No. 3:18-CV-02090 (N.D. Cal.) (filed Apr. 5, 2018) (Kim, M.J.)

viii. *Price v. Facebook, Inc.*, No. 3:18-CV-01732 (N.D. Cal.) (filed Mar. 20, 2018) (Chhabria, J.)

ix. *Rubin v. Facebook, Inc.*, No. 3:18-CV-01852 (N.D. Cal.) (filed Mar. 26, 2018) (Spero, M.J.)

b. **Northern District of Illinois**: *Comforte v. Cambridge Analytica*, No. 1:18-CV-02120 (N.D. Ill.) (filed Mar. 22, 2018) (Bucklo, J.)

c. **Southern District of Texas**: *Lodowski v. Facebook, Inc.*, No. 4:18-CV-00907 (S.D. Tex.) (filed Mar. 23, 2018) (Ellison, J.)

d. **District of New Jersey**: *Malskoff v. Facebook, Inc.*, No. 2:18-CV-04451 (D.N.J.) (filed Mar. 27, 2018) (Salas, J.).

e. **Central District of California:** *O'Hara v. Facebook, Inc.*, No. 8:18-CV-00571 (C.D. Cal.) (filed Apr. 4, 2018) (unassigned)

f. **Northern District of Alabama:** *Williams v. Facebook, Inc.*, No. 2:18-CV-00535-RDP (N.D. Ala.) (filed Apr. 4, 2018) (Proctor, J.)

The consumer class actions substantially overlap in many ways. Each seeks recovery on behalf of Facebook accountholders whose data allegedly was obtained by Cambridge Analytica

via Kogan's app, "thisisyourdigitallife." (*See* Appendix B.)[4] All of the complaints name Facebook and Cambridge Analytica as defendants, and five actions—*Lodowski*, *Malskoff*, *Rubin*, *Kooser*, and *O'Hara*—also name either Kogan or GSR.[5]

There is also substantial overlap among the legal theories and causes of action asserted in the various complaints. (*See* Appendix C.) Twelve actions—*Lodowski*, *Malskoff*, *O'Kelly*, *Price*, *Rubin*, *Beiner*, *Haslinger*, *Kooser*, *O'Hara*, *Williams*, *Labajo*, and *Picha*—allege violations of state consumer protection laws.[6] All allege state common-law torts and/or related privacy-law claims.[7] Eleven—*Comforte*, *Gennock*, *Lodowski*, *Malskoff*, *Beiner*, *Haslinger*, *Kooser*, *O'Hara*, *Williams*, *Labajo*, and *Picha*—allege federal causes of action under the Stored Communications Act, 18 U.S.C. § 2701, *et seq.*, or the Wiretap Act, 18 U.S.C. §2510, *et seq.* And all center around the same operative theories of wrongdoing: that Cambridge Analytica and other actors wrongfully

---

4 *See also Price*, Compl. ¶ 24; *Rubin*, Compl. ¶ 41; *Gennock*, Compl. ¶ 60; *O'Kelly*, Compl. ¶ 36; *Comforte*, Compl. ¶¶ 230-43; *Lodowski*, Compl. ¶ 27; *Beiner*, Compl. ¶ 68; *Malskoff*, Compl. ¶ 70; *Haslinger*, Compl. ¶ 36; *Kooser*, Compl. ¶ 40; *O'Hara*, Compl. ¶¶ 92-93; *Williams*, Compl. ¶¶ 29-30; *Picha*, Compl. ¶ 86; *Labajo*, Compl. ¶¶ 88-89.

5 The *Rubin* and *Kooser* complaints also name Cambridge Analytica's parent entity, SCL Group, and the *Comforte* complaint names Mark Zuckerberg, Facebook's CEO. The *Lodowski* and *Malskoff* complaints name Robert Mercer, a hedge fund manager who reportedly owned Cambridge Analytica. The *O'Hara* complaint also names Stephen Bannon.

6 Cal. Bus. & Prof. Code § 17200 (*Lodowski*, *Malskoff*, *O'Kelly*, *Price*, *Rubin*, *Beiner*, *Haslinger*, *O'Hara*, *Labajo*, and *Picha*); Illinois Consumer Fraud & Deceptive Practices Act, 815 ILCS 505 (*Comforte*); N.J. Consumer Fraud Act, N.J. Stat. Ann. § 56:8-1 (*Malskoff*); Ala. Deceptive Trade Practices Act, Ala. Code § 8-19-1 (*Williams*).

7 Negligence (*Comforte*, *Lodowski*, *Malskoff*, *O'Kelly*, *Price*, *Rubin*, *Haslinger*, *Kooser*, *O'Hara*, *Williams*, *Labajo*, and *Picha*); invasion of privacy, under several theories (*Comforte*, *Gennock*, *O'Kelly*, *Rubin*, *Beiner*, *Haslinger*, *Kooser*, *O'Hara*, and *Picha*); conversion (*Beiner*, *Kooser*, *O'Hara*, *Williams*, and *Picha*); civil conspiracy (*Beiner*, *Kooser*, and *Williams*); fraudulent misrepresentation (*O'Kelly* and *Kooser*), and misappropriation of valuable property without compensation (*Labajo*).

exploited Facebook's platform to obtain data that they used for unauthorized purposes, and that Facebook should have done more to prevent these wrongs by imposing more robust controls on the use of data by third party apps. The nearly identical factual allegations all appear to be copied from the same two news reports—the March 17, 2018, articles in *The New York Times* and *The Guardian*. (*See* Appendix A.)

The class allegations in all of the actions also substantially overlap: although the class definitions vary slightly, all seek to certify nationwide classes of Facebook accountholders whose data was obtained by Cambridge Analytica and used without or beyond authorization. (*See* Appendix B.) And all of the putative classes suffer from the same weaknesses that, in Facebook's view, will make class certification impossible, including the common struggle to identify any cognizable theory of injury or damages, and the myriad individualized issues, including issues of consent, that will predominate over any classwide concerns. It is imperative for class certification proceedings to be handled in a coordinated manner in a single MDL proceeding.

Finally, all of these actions are in their nascent stages. Many of the complaints have not yet been served; no pleadings or other papers beyond the complaints have been filed; and the courts have expended few if any resources.

On March 30, 2018, the *Beiner* plaintiffs moved to establish an MDL in the Northern District of California for all of the consumer class actions. Dkt. 1. That same day, the *Lodowski* plaintiffs cross-moved to establish an MDL over the same actions in the Southern District of Texas.

Dkts. 5, 11, and the *Rubin* plaintiffs filed a response supporting the *Beiner* plaintiffs' request for an MDL in the Northern District of California, Dkt. 7.[8]

III. ARGUMENT

A. The Fourteen Consumer Class Actions Should Be Transferred Into An MDL.

Consolidation or coordination of pretrial proceedings in an MDL is appropriate if (1) actions pending in different federal courts involve "one or more common questions of fact"; and (2) consolidation "will be for the convenience of parties and witnesses and will promote the just and efficient conduct of such actions." 28 U.S.C. § 1407(a). Facebook agrees with the moving plaintiffs that both factors strongly favor consolidation of the pretrial proceedings of these actions.

1. *The Actions Involve Overlapping Factual Allegations.*

Section 1407 requires that the cases to be consolidated raise "one or more common questions of fact."[9] It does not require that the cases be identical in every respect. "[T]ransfer under Section 1407 does not require a complete identity or even majority of common factual issues as a prerequisite to transfer." *In re Ins. Brokerage Antitrust Litig.*, 360 F. Supp. 2d 1371, 1372 (J.P.M.L. 2005). The actions at issue here plainly satisfy this requirement.

---

[8] Since those motions were filed, six new consumer class actions were filed in the Northern and Central Districts of California and the Northern District of Alabama: the *Haslinger*, *Kooser*, *O'Hara*, *Williams*, *Labajo*, and *Picha* cases, included in the list above, all of which should be included in any MDL proceeding. Facebook has accordingly filed a Notice of Related Actions to include those first four actions in this MDL, Dkt. 13, and is concurrently filing a Notice of Related Actions regarding *Labajo* and *Picha*.

[9] Of course, this inquiry is very different from the class certification question required by Rule 23. *See, e.g., In re Trade Partners, Inc., Inv'rs Litig.*, 493 F. Supp. 2d 1381 (J.P.M.L. 2007) (centralization under Section 1407 appropriate even where individual questions of fact and law predominate for class certification purposes). Facebook reserves all of its defenses and objections to class certification, including, the absence of common questions susceptible to common answers (*see Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011)), and the fact that common questions do not predominate over individualized questions. *See* Fed. R. Civ. P. 23(b)(3); *Comcast Corp. v. Behrend*, 133 S. Ct. 1426, 1436–37 (2013).

The consumer class actions at issue here present many "common question[s] of fact." 28 U.S.C. § 1407(a). As set out above, all of the actions stem from the same alleged factual predicate—Cambridge Analytica's unauthorized use of Facebook users' data—and propose identical or overlapping nationwide classes. Factual issues central to class certification, liability, and damages will be similar across all the cases. For example, the manner in which Kogan, GSR, and Cambridge Analytica misused the Facebook platform and misrepresented its activities to Facebook is a common issue in all actions that will be critical to determining proximate causation and liability.

As a result of this substantial overlap, the cases will present substantially similar issues at the motion to dismiss, class certification, and summary judgment phases.

2. *Consolidation Will Serve "The Convenience Of The Parties And Witnesses" And "Promote The Just And Efficient Conduct Of The Actions."*

Consolidation pursuant to Section 1407(a) also would be more convenient for the parties and efficient for the judicial system, for two principal reasons:

First, litigating these cases separately would impose substantial and duplicative discovery burdens. The Panel consistently has held that transfer under Section 1407 is intended to prevent such duplication. *See, e.g.*, *In re Starmed Health Pers. FLSA Litig.*, 317 F. Supp. 2d 1380, 1381 (J.P.M.L. 2004) (consolidating two actions in part because transfer was necessary to "eliminate duplicative discovery" and "conserve the resources of the parties").[10] That is especially so where,

---

[10] *See also In re Zyprexa Prods. Liab. Litig.*, 314 F. Supp. 2d 1380, 1382 (J.P.M.L. 2004) ("[T]ransfer under Section 1407 will offer the benefit of placing all actions in this docket before a single judge who can structure pretrial proceedings to consider all parties' legitimate discovery needs while ensuring that common parties and witnesses are not subjected to discovery demands that duplicate activity that will occur or has already occurred in other actions."); *In re Enron Corp. Sec., Deriv. & ERISA Litig.*, 196 F. Supp. 2d 1375, 1376–77 (J.P.M.L. 2002) (consolidating multiple actions because of the cases' strong connection to Southern District of Texas, where Enron was headquartered, witnesses were located, and auditors performed their work).

as here, the cases are numerous, are pending in several different districts, and are likely to be followed by additional actions. *See, e.g., In re Schnuck Markets, Inc., Customer Data Sec. Breach Litig.*, 978 F. Supp. 2d 1379, 1380–81 (J.P.M.L. 2013) (centralizing cases because there was no "reasonable prospect" that Section 1404 transfer would "eliminate the multidistrict character of the litigation").

Because all of the actions concern the same factual core, discovery in the fourteen actions is likely to be virtually identical, including the same witnesses, the same documentary evidence, and the same third party discovery. "Allowing the witnesses to appear once in a single venue is more convenient that requiring them to appear multiple times in multiple venues." *Cluck v. IKON Office Sols., Inc.*, No. 11-05027-JSW, 2012 WL 1610789, at *2 (N.D. Cal. May 8, 2012). As the Panel has recognized, only centralization can achieve this goal: "informal coordination and cooperation among the parties and courts" is not "sufficient to eliminate the potential for duplicative discovery, inconsistent pretrial rulings, and conflicting discovery obligations." *In re Generic Pharm. Pricing Antitrust Litig.*, No. MDL 2724, 2017 WL 4582710, at *2 (J.P.M.L. Aug. 3, 2017). Similarly, it is appropriate to grant centralization now, without forcing the parties to litigate multiple change of venue motions, given the numerous tag along actions that likely will be filed in the coming weeks or months. *In re: Gerber Probiotic Prod. Mktg. & Sales Practices Litig.*, 899 F. Supp. 2d 1378, 1381 (J.P.M.L. 2012).

Second, centralization will eliminate the risk of inconsistent pretrial rulings on discovery, dispositive motions, and other pretrial matters. *See, e.g., In re Pineapple Antitrust Litig.*, 342 F. Supp. 2d 1348, 1349 (J.P.M.L. 2004) (consolidating cases to "prevent inconsistent pretrial rulings"). That risk is especially acute in putative class actions with overlapping class definitions, as is the case here. Where there is such "overlap," ["[c]entralization in one district will bring

efficiencies to the pretrial proceedings of these actions and will eliminate duplicative discovery and prevent inconsistent pretrial rulings, particularly with respect to class certification." *In re Imprelis Herbicide Mktg., Sales Practices & Prod. Liab. Litig.*, 825 F. Supp. 2d 1357, 1359 (J.P.M.L. 2011); *accord, e.g., In re Toys 'R' Us-Delaware, Inc., FACTA Litig.*, 581 F. Supp. 2d 1377, 1377–78 (J.P.M.L. 2008) (centralization will "eliminate duplicative discovery; prevent inconsistent pretrial rulings, especially with respect to class certification; and conserve the resources of the parties, their counsel and the judiciary"); *In re Sierra Wireless, Inc., Sec. Litig.*, 387 F. Supp. 2d 1363, 1364 (J.P.M.L. 2005) (same); *In re High Sulfur Content Gasoline Prods. Liab. Litig.*, 344 F. Supp. 2d 755, 757 (J.P.M.L. 2004) (same). Indeed, Section 1407 was "designed" to prevent the "pretrial chaos" resulting from "conflicting class action determinations." *In re Plumbing Fixture Cases*, 298 F. Supp. 484, 492–93 (J.P.M.L. 1968).

Such chaos is especially likely where proposed classes overlap because the first case to reach judgment could trigger res judicata consequences for putative class members in other cases; plaintiffs "would thus necessarily be in destabilizing competition to race to an early resolution." *In re Facebook, Inc., IOP Sec. & Derivative Litig.*, No. 12-CV-4081, 2013 WL 4399215, *5 (S.D.N.Y. Aug. 13, 2013). "Such conflicts are avoided by having … a single consolidated action on behalf of a unitary putative class." *Id.* Here, the putative classes are virtually identical, making the risk of conflicting rulings absent consolidation particularly acute.

Different federal courts also could reach contradictory rulings on other core legal issues. It will be critical for these issues to be adjudicated in a streamlined and consistent fashion.

In short, these actions involve a significant number of overlapping (and often identical) factual allegations, legal claims, and putative class members. Allowing them to proceed separately through the pretrial process would create a significant risk of inconsistent pretrial rulings on a wide

range of issues that could lead to inconsistent outcomes, including for members of the same putative classes whose interests are ostensibly represented in multiple jurisdictions. *See In re Texas Gulf Sulphur Sec. Litig.*, 344 F. Supp. 1398, 1400 (J.P.M.L. 1972) ("We have frequently held that the possibility of inconsistent class action determinations is an important factor favoring transfer."); *In re Sugar Indus. Antitrust Litig.*, 395 F. Supp. 1271, 1273 (J.P.M.L. 1975) (consolidation necessary for actions with "overlap[ping] or duplicat[ive]" class allegations). Centralization would prevent such inconsistency.

Centralization is particularly appropriate because none of these actions has moved past the pleadings stage. No answers or motions to dismiss have been filed, no Rule 26(f) conferences have been held, and no discovery has taken place. *See, e.g., In re Int'l House of Pancakes Franchise Litig.*, 374 F. Supp. 1406, 1407 (J.P.M.L. 1974) (transfer appropriate where discovery not well-advanced). The cases should be consolidated in a single transferee district.

3. *Establishing An MDL Now Is The Most Efficient Way To Bring These Cases Together.*

In its briefing order, the Panel asked the parties to "address what steps they have taken to pursue alternatives to centralization." Dkt. 3. As noted above, all of the securities and derivative cases to date have been filed in the Northern District of California, and the plaintiffs in the securities cases are taking steps to relate all of the cases to a single judge, the Honorable Edward J. Davila. Indeed, the very first-filed case of all three categories of cases (securities, derivative, and consumer) is assigned to Judge Davila. *See Yuan*, No. 5:18-CV-01725 (N.D. Cal.) (filed Mar. 20, 2018). As for the consumer cases, the parties who have spoken on the issue appear to agree that an MDL is the most efficient and effective means of avoiding duplication in these cases, which currently are pending in six different judicial districts. Any effort at informal coordination and scheduling among these cases will not eliminate the near-certain risk of conflicting or competing

rulings on motions to dismiss or for class certification. Trying to transfer all of the cases to one district also would be time-consuming and possibly ineffectual. Already, different plaintiffs' counsel have asserted different positions to the Panel on where the MDL should be located, and it is unlikely that the same parties could achieve a voluntary transfer of the actions to a single judicial district. And litigating multiple contested transfer motions would be unnecessarily time-consuming and, given the discretionary nature of 28 U.S.C. § 1404, would provide no guarantee that the actions actually would end up in a single district. Extending the proceedings in this way would be burdensome to the parties and the judicial system, would not accomplish the immediate coordination of motion practice and discovery that Facebook believes is essential, and would be inconsistent with the urgent action that plaintiffs have asserted is necessary to resolve this litigation. Dkt. 7 at 2.

B. The Actions Should Be Transferred To The Northern District Of California.

In selecting an appropriate transferee district, the Panel considers multiple factors: where most discovery will take place; where the relevant conduct occurred; the procedural stage of each case; and where the plurality of cases have been filed. *See, e.g., In re Treasury Sec. Auction Antitrust Litig.*, 148 F. Supp. 3d 1360, 1361–62 (J.P.M.L. 2015) (transferring to Southern District of New York because all defendants were headquartered there and most of the cases had been filed in that district); *In re Nat'l Football League's "Sunday Ticket" Antitrust Litig.*, 148 F. Supp. 3d 1358, 1359–60 (J.P.M.L. 2015) (transferring to Central District of California because 15 actions had been filed there, defendant maintained its headquarters there, and common evidence would likely be found there).

These factors strongly favor the Northern District of California. That district is home to Facebook's headquarters, so any discovery relating to its operations and the use of its platform would likely be conducted there. It also is where the majority of the consumer class actions (nine

of fourteen) have been filed, and where all of the related shareholder litigation (securities and derivative actions) is pending.

1. *Relevant U.S.-Based Documents And Witnesses Are Likely Located In The Northern District Of California.*

One factor the Panel considers in selecting an appropriate transferee district is the location where most discovery will take place and where the relevant conduct occurred. *See, e.g., In re AMF Computerized Cash Register Contract Litig.*, 360 F. Supp. 1404, 1405 (J.P.M.L. 1973). Here, discovery likely will center around events in the U.K. (where Kogan resides and where Cambridge Analytica's relevant office is located) and the Northern District of California (where Facebook is headquartered). Aleksandr Kogan and Cambridge Analytica are the parties responsible for misappropriating consumer data and violating Facebook's terms of service. Kogan is a U.K. resident who apparently operated out of the U.K. Cambridge Analytica is based in New York, but its corporate parent, SLC, is a U.K. company, and the recent investigations by U.K. data regulators have focused on Cambridge Analytica's London offices, suggesting that the relevant documents and witnesses will be located there.[11] To the extent discovery focuses on Facebook's operations, the misuse of its platform and data, and the controls that Facebook had in place, that discovery will be centered in the Northern District of California, where Facebook is based and most of its relevant witnesses reside. Indeed, the Panel previously assigned Facebook privacy litigation to the Northern District of California because "[c]ommon defendant Facebook is headquartered in the Northern District of California, where relevant documents and witnesses are located." *In re Facebook Internet Tracking Litig.*, 844 F. Supp. 2d 1374, 1375 (J.P.M.L. 2012).

---

[11] H. Summers & N. Slawson, Investigators complete seven-hour Cambridge Analytica HQ search, The Guardian (Mar. 24, 2018), https://www.theguardian.com/news/2018/mar/23/judge-grants-search-warrant-for-cambridge-analyticas-offices.

In this case, too, many Facebook witnesses whom plaintiffs might seek to depose work at Facebook's headquarters in Menlo Park, in the Northern District of California.

2. *No Case Has Advanced Past The Filing Of A Complaint.*

This Panel also considers the degree of procedural advancement of the pending cases in selecting a transferee district. *See, e.g., In re Air Crash near Peixoto De Azevada, Brazil on Sept. 29, 2006*, 493 F. Supp. 2d 1374, 1376 (J.P.M.L. 2007) (selecting a transferee district in part because actions pending in the district were "more procedurally advanced than the actions pending elsewhere"). Here, although all of the pending cases are in their nascent stages, the first case (*Price*) was filed in the Northern District of California. All cases were filed within the last three weeks, Facebook has filed no answers or motions to dismiss, no court has held a Rule 26(f) conference, and no discovery has taken place.

3. *Actions Have Been Filed In Districts Across The Country, With The Largest Number Filed In The Northern District Of California.*

The Panel also considers the prevalence of the member actions in the candidate districts. *See, e.g., In re PepsiCo, Inc., Bottled Water Mktg. & Sales Practices Litig.*, 560 F. Supp. 2d 1348, 1349 (J.P.M.L. 2008) (selecting a transferee district in part because two of four filed actions were already pending there); *In re Fosamax Prods. Liab. Litig.*, 444 F. Supp. 2d 1347, 1349–50 (J.P.M.L. 2006) (15 of 19 actions already pending in transferee district); *In re Holiday Magic Sec. & Antitrust Litig.*, 368 F. Supp. 806, 807 (J.P.M.L. 1973) (per curiam) (two of five cases already pending in transferee district).

Here, plaintiffs have filed actions against Facebook in six districts across the country. Nine actions were filed in the Northern District of California. One action was filed in each of the Southern District of Texas, the Northern District of Illinois, the District of New Jersey, the Central District of California, and the Northern District of Alabama. That so many plaintiffs have filed

their cases in the Northern District of California is a strong indication that their counsel view that district as being appropriate for these actions.

In addition, all of the various securities class actions and shareholder derivative actions that have been filed in the wake of the same news articles are already pending in the Northern District of California, and two of the three securities class actions are pending before Judge Edward J. Davila (the plaintiffs in those cases are in the process of consolidating the third such action with Judge Davila as well). *Cf. In re: Apple, Inc. Device Performance Litig.*, MDL No. 2827, Dkt. 40, at 2 (J.P.M.L. Apr. 4, 2018) (assigning MDL to Judge Davila because he "already ha[d] taken steps to coordinate the actions before him"). These shareholder actions center around the same operative set of underlying facts pertaining to Cambridge Analytica, such that any discovery in those proceedings will necessarily overlap with discovery in the consumer actions. Litigation in the same district would give the transferee court substantial opportunities to achieve efficiencies not only across the consumer classes, but also in the broader litigation, particularly if the same judge is assigned to all actions. This factor, too, suggests that the Northern District of California is the appropriate center of gravity for consolidated proceedings.

4. *Transfer To The Southern District of Texas Would Not Further The Interests Of Multidistrict Litigation.*

In contrast, transfer to the Southern District of Texas would not further the interests of MDL consolidation. Only one action was filed in that district and, to Facebook's knowledge, none of the relevant documents or witnesses will be located in Texas. The *Lodowski* plaintiffs point to Houston's geographic location in the center of the country as being beneficial. Dkt. 11-1 at 5-7. But Houston's relative proximity to the east coast is substantially outweighed by the travel burdens that would be imposed on all California-based witnesses, as well as counsel in

most of the cases. And, as the *Beiner* and *Rubin* plaintiffs point out, travel in and out of the San Francisco Bay Area is very easy, facilitated by three international airports.

IV. CONCLUSION

For the foregoing reasons, consolidation of these actions into a multidistrict litigation for pretrial proceedings would further "the convenience of parties and witnesses and promote the just and efficient conduct of [the] actions." 28 U.S.C. § 1407(a). Facebook respectfully requests that this Panel grant the pending motion to establish an MDL covering the actions listed on the schedule attached to the *Beiner* plaintiff's motion and the actions identified in Facebook's Notices of Related Actions and assign the MDL to the Northern District of California for consolidated pretrial proceedings.

Dated: April 6, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Orin Snyder*

Orin Snyder
200 Park Avenue
New York, N.Y. 10166
Tel: 212.351.2400
Fax: 212.351.6335
osnyder@gibsondunn.com

Joshua S. Lipshutz
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202.955.8217
Fax: 202.530.9614
jlipshutz@gibsondunn.com

Kristin A. Linsley
Brian M. Lutz
555 Mission Street
Suite 300
San Francisco, CA 94105
Tel: 415.393.8379
Fax: 415.374.8474
klinsley@gibsondunn.com
blutz@gibsondunn.com

Attorneys for Facebook, Inc.

APPENDIX A

All Complaints Rely on The March 17, 2018, *New York Times* and *Guardian* Articles

- M. Rosenberg, N. Confessore & C. Cadwalladr, *How Trump "Consultants" Exploited the Facebook Data of Millions*, N.Y. Times (Mar. 17, 2018)
- C. Cadwalladr & E. Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian (Mar. 17, 2018), https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Beiner v. Facebook, Inc., No. 3:18-CV-1953 (N.D. Cal.) (filed Mar. 29, 2018) (Corley, M.J.)	New York Times article cited in Compl. ¶¶ 24 n.13, 45 n.27, 48 n.30, 49 n.31. Guardian article cited in Compl.¶ 32 n.17.
Comforte v. Cambridge Analytica, No. 1:18-CV-02120 (N.D. Ill.) (filed Mar. 22, 2018) (Bucklo, J.)	"[Christopher] Wylie told *The New York Times* that he had access to the Facebook profiles which 'contained enough information, including places of residence, that [Cambridge] could match users to other records and build psychographic profiles.' Wylie told *The New York Times* that Cambridge's access to 'the Facebook data…was "the saving grace" that let his team deliver the models it had promised the Mercers.'" Compl. ¶¶ 35-36.
Gennock v. Facebook, Inc., No. 3:18-CV-01891 (N.D. Cal.) (filed Mar. 27, 2018) (Ryu, M.J.)	"*The Guardian* published an article, based on information obtained from, *inter alia*, Mr. Wylie, which detailed Cambridge's unauthorized mining of 50,000,000 Facebook users' data and its employment of that data to target individuals with its psychological operations to influence their views regarding the 2016 Presidential Election." Compl. ¶ 49.

Haslinger v. Facebook, Inc., No. 3:18-CV-01984 (N.D. Cal.) (filed Mar. 30, 2018) (Rogers, J.)	"On March 17, 2018, both the *New York Times* and *The Guardian* reported that Cambridge Analytica had obtained Facebook users' Personal Information from Facebook, without the users' permission ('Data Breach'). The reports revealed that Cambridge Analytica used the data of 50 million people obtained from Facebook for political purposes, without proper disclosures or permission." Compl. ¶ 14.
Kooser v. Facebook, Inc., No. 3:18-CV-02009 (N.D. Cal.) (filed Apr. 2, 2018) (Laporte, M.J.)	"On March 17, 2018, both the *New York Times* and *The Guardian* reported on CA's use of Personal Information obtained from Facebook without permission, and under the pretext of claiming to be collecting and using it for academic purposes. The reports revealed that Cambridge Analytica, a firm brought on by presidential campaigns to target voters online, used the data of 50 million people obtained from Facebook without proper disclosures or permission." Compl. ¶ 14.
Labajo v. Facebook, Inc., No. 4:18-CV-02093 (N.D. Cal.) (filed Apr. 5, 2018) (Westmore, M.J.)	"On March 17, 2018, the *New York Times* and *The Guardian* reported that Cambridge Analytica had gained access to the "harvested" Personal Information of more than 50 million Facebook users, which had been taken in a massive data breach in 2014. The stolen information was, among other things, used to construct psychological profiles of the Facebook users, so that they could be targeted with advertising in an attempt to influence their voting in the 2016 presidential election." Compl. ¶ 5.
Lodowski v. Facebook, Inc., No. 4:18-CV-00907 (S.D. Tex.) (filed Mar. 23, 2018) (Ellison, J.)	Citing a related article published in the Guardian: "On March 18, 2018, the Guardian published a report on CA [Cambridge Analytica]. The report explains an elaborate voter targeting program developed and used by CA to influence voter preferences in the 2016 presidential election for the United States for the benefit of then candidate Donald Trump. The Guardian's report details CA's voter targeting techniques using information the newspaper acquired from a whistleblower named Christopher Wylie. "Wylie has personal knowledge of the scheme, because he was a lead engineer in the project and was employed by CA. Wylie explained the scheme in detail. "According to the report, CA used a massive database, filled with Facebook users' surreptitiously acquired Facebook data, to target voters with information that was designed to manipulate or influence their voting preferences. Wylie further explained that data in the database was acquired with the assistance of a Cambridge University professor named Aleksandr Kogan." Compl. ¶¶ 13-15.

Malskoff v. Facebook, Inc., No. 2:18-CV-04451 (D.N.J.) (filed Mar. 27, 2018) (Salas, J.)	"On March 17, 2018, The New York Times and The Guardian reported that Cambridge Analytica still possesses data it inappropriately gathered from as many as 50 million Facebook users. Only after the reports were published, Facebook suspended Cambridge Analytica (and Wylie, the very whistleblower who revealed the fraudulent scheme to the public)." Compl. ¶ 56.
O'Hara v. Facebook, Inc., No. 8:18-CV-00571 (C.D. Cal.) (filed Apr. 4, 2018) (unassigned)	Guardian article cited in Compl.¶¶ 42 n.14, 66 n.37
O'Kelly v. Facebook, Inc., No. 3:18-CV-01915 (N.D. Cal.) (filed Mar. 28, 2018) (Laporte, M.J.)	"On March 17, 2018, The New York Times published an investigative report entitled 'How Trump Consultants Exploited the Facebook Data of Millions,' revealing that Cambridge Analytica used the data of 50 million people." Compl. ¶ 27.
Picha v. Facebook, Inc., No. 3:18-CV-02090 (N.D. Cal.) (filed Apr. 5, 2018) (Kim, M.J.)	"On March 17, 2018, both the *New York Times* and *The Guardian* reported on Cambridge Analytica's use of PII obtained from Facebook without permission, and under the pretext of claiming to be collecting and using it for academic purposes. The reports revealed that Cambridge Analytica, a firm hired by the Trump campaign to target voters online, used the data of 87 million people obtained from Facebook without proper disclosures or permission." Compl. ¶ 24.
Price v. Facebook, Inc., No. 3:18-CV-01732 (N.D. Cal.) (filed Mar. 20, 2018) (Chhabria, J.)	"On March 17, 2018, both the *New York Times* and *The Guardian* reported on CA's use of Personal Information obtained from Facebook without permission, and under the pretext of claiming to be collecting and using it for academic purposes. The reports revealed that Cambridge Analytica, a firm brought on by the Trump campaign to target voters online, used the data of 50 million people obtained from Facebook without proper disclosures or permission." Compl. ¶ 10.
Rubin v. Facebook, Inc., No. 3:18-CV-01852 (N.D. Cal.) (filed Mar. 26, 2018) (Spero, M.J.)	"On March 17, 2018, the Guardian reported, based on information provided by Christopher Wylie, a co-founder of CAMBRIDGE, that dating back to at least 2014, Defendants SCL, CAMBRIDGE and GSR obtained from FACEBOOK the private information of at least 50 million American FACEBOOK users who did not consent to their information being shared with SCL, CAMBRIDGE, or any other related companies or individuals." Compl. ¶ 15.

Williams v. Facebook, Inc., No. 2:18-cv-00535 (N.D. Ala.) (filed Apr. 4, 2018) (Proctor, J.)	New York Times article cited in Compl. ¶ 20 n.11 Guardian article cited in Compl. ¶ 17 n.8

APPENDIX B
Proposed Class Definitions

Beiner v. Facebook, Inc., No. 3:18-CV-1953 (N.D. Cal.) (filed Mar. 29, 2018) (Corley, M.J.)	"All persons who registered for Facebook accounts in the United States and whose Personal Information was obtained by app developers through the 'friends permission' functionality." Compl. ¶ 68.
Comforte v. Cambridge Analytica, No. 1:18-CV-02120 (N.D. Ill.) (filed Mar. 22, 2018) (Bucklo, J.)	No express class definition. "Plaintiffs and similarly situated Class Members were harmed by the misconduct of Cambridge, Facebook and the John Does Defendants to the extent that they had their personal information mined as a result of another Facebook 'friend' downloading and using the *MyDigitalLife* app." Compl. ¶ 119
Gennock v. Facebook, Inc., No. 3:18-CV-01891 (N.D. Cal.) (filed Mar. 27, 2018) (Ryu, M.J.)	"CLASS: All Facebook users in the United States whose personal information was acquired by Cambridge through use of the YDL App. "CALIFORNIA SUBCLASS: All Facebook users in California whose personal information was acquired by Cambridge through use of the YDL App. "PENNSYLVANIA SUBCLASS: All Facebook users in Pennsylvania whose personal information was acquired by Cambridge through use of the YDL App." Compl. ¶ 60.
Haslinger v. Facebook, Inc., No. 3:18-CV-01984 (N.D. Cal.) (filed Mar. 30, 2018) (Rogers, J.)	"All natural persons in the United States who registered for Facebook accounts and whose Personal Information was obtained from Facebook by Cambridge Analytica or other entities without authorization or in excess of authorization." Compl. ¶ 36.

Kooser v. Facebook, Inc., No. 3:18-CV-02009 (N.D. Cal.) (filed Apr. 2, 2018) (Laporte, M.J.)	"All persons who own Facebook accounts in the United States and whose Personal Information was obtained by Defendants CA, SCL and/or GSR.." Compl. ¶ 40.
Labajo v. Facebook, Inc., No. 4:18-CV-02093 (N.D. Cal.) (filed Apr. 5, 2018) (Westmore, M.J.)	"All Facebook users in the United States whose Facebook profile information was acquired by Cambridge Analytica in June-August 2014." Compl. ¶ 88. "All Facebook users in the United States whose personal or profile information was taken by third parties using Facebook search tools." Compl. ¶ 89.
Lodowski v. Facebook, Inc., No. 4:18-CV-00907 (S.D. Tex.) (filed Mar. 23, 2018) (Ellison, J.)	"All persons who registered for Facebook accounts in the United States and whose Personal Information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 27.
Malskoff v. Facebook, Inc., No. 2:18-CV-04451 (D.N.J.) (filed Mar. 27, 2018) (Salas, J.)	"All persons who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 70. "All New Jersey residents who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 71. "All California residents who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 72.
O'Hara v. Facebook, Inc., No. 8:18-CV-00571 (C.D. Cal.) (filed Apr. 4, 2018) (unassigned)	"All persons in the United States with Facebook accounts whose personal information was obtained by Cambridge Analytica, LLC without or in excess of authorization." Compl. ¶ 92. "All residents in the State of California with Facebook accounts whose personal information was obtained by Cambridge Analytica, LLC without or in excess of authorization." Compl. ¶ 93.

O'Kelly v. Facebook, Inc., No. 3:18-CV-01915 (N.D. Cal.) (filed Mar. 28, 2018) (Laporte, M.J.)	"All persons who registered for Facebook accounts in the United States and whose personal information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 36.
Picha v. Facebook, Inc., No. 3:18-CV-02090 (N.D. Cal.) (filed Apr. 5, 2018) (Kim, M.J.)	"All persons who registered for a Facebook account in the United States whose Personally Identifiable Information was obtained from Facebook by Cambridge Analytica, or other entities, without authorization or in excess of authorization." Compl. ¶ 86.
Price v. Facebook, Inc., No. 3:18-CV-01732 (N.D. Cal.) (filed Mar. 20, 2018) (Chhabria, J.)	"All persons who registered for Facebook accounts in the United States and whose Personal Information was obtained from Facebook by Cambridge Analytica without authorization or in excess of authorization." Compl. ¶ 24.
Rubin v. Facebook, Inc., No. 3:18-CV-01852 (N.D. Cal.) (filed Mar. 26, 2018) (Spero, M.J.)	"All persons in the United States whose personal data was stored by FACEBOOK and who had such data accessed by GSR, SCL, or CAMBRIDGE without authorization or in excess of authorization." Compl. ¶ 41.
Williams v. Facebook, Inc., No. 2:18-cv-00535 (N.D. Ala.) (filed Apr. 4, 2018) (Proctor, J.)	"All individuals in the United States who registered for Facebook accounts and whose Personal Information was obtained from Facebook without authorization or in excess of authorization." Compl. ¶ 29. "All individuals in Alabama who registered for Facebook accounts and whose Personal Information was obtained from Facebook without authorization or in excess of authorization." Compl. ¶ 30.

APPENDIX C
Causes of Action

Case	State Privacy & Property Torts	State Consumer Protection Statutes	Negligence	Federal Statutory (RICO, Stored Communications Act, Wiretap Act)	Breach of Contract & Unjust Enrichment
Beiner v. Facebook, Inc., No. 3:18-CV-1953 (N.D. Cal.) (filed Mar. 29, 2018) (Corley, M.J.)	X	X		X	
Comforte v. Cambridge Analytica, No. 1:18-CV-02120 (N.D. Ill.) (filed Mar. 22, 2018) (Bucklo, J.)	X	X	X	X	X
Gennock v. Facebook, Inc., No. 3:18-CV-01891 (N.D. Cal.) (filed Mar. 27, 2018) (Ryu, M.J.)	X			X	
Haslinger v. Facebook, Inc., No. 3:18-CV-01984 (N.D. Cal.) (filed Mar. 30, 2018) (Rogers, J.)	X	X	X	X	X

Case	State Privacy & Property Torts	State Consumer Protection Statutes	Negligence	Federal Statutory (RICO, Stored Communications Act, Wiretap Act)	Breach of Contract & Unjust Enrichment
Kooser v. Facebook, Inc., No. 3:18-CV-02009 (N.D. Cal.) (filed Apr. 2, 2018) (Laporte, M.J.)	X	X	X	X	X
Labajo v. Facebook, Inc., No. 4:18-CV-02093 (N.D. Cal.) (filed Apr. 5, 2018) (Westmore, M.J.)	X	X	X	X	X
Lodowski v. Facebook, Inc., No. 4:18-CV-00907 (S.D. Tex.) (filed Mar. 23, 2018) (Ellison, J.)	X		X	X	
Malskoff v. Facebook, Inc., No. 2:18-CV-04451 (D.N.J.) (filed Mar. 27, 2018) (Salas, J.)	X	X	X	X	X
O'Hara v. Facebook, Inc., No. 8:18-CV-00571 (C.D. Cal.) (filed Apr. 4, 2018) (unassigned)	X	X	X	X	X

Case	State Privacy & Property Torts	State Consumer Protection Statutes	Negligence	Federal Statutory (RICO, Stored Communications Act, Wiretap Act)	Breach of Contract & Unjust Enrichment
O'Kelly v. Facebook, Inc., No. 3:18-CV-01915 (N.D. Cal.) (filed Mar. 28, 2018) (Laporte, M.J.)	X	X	X		X
Picha v. Facebook, Inc., No. 3:18-CV-02090 (N.D. Cal.) (filed Apr. 5, 2018) (Kim, M.J.)	X	X	X	X	
Price v. Facebook, Inc., No. 3:18-CV-01732 (N.D. Cal.) (filed Mar. 20, 2018) (Chhabria, J.)		X	X		
Rubin v. Facebook, Inc., No. 3:18-CV-01852 (N.D. Cal.) (filed Mar. 26, 2018) (Spero, M.J.)	X	X	X	X	
Williams v. Facebook, Inc., No. 2:18-cv-00535 (N.D. Ala.) (filed Apr. 4, 2018) (Proctor, J.)	X	X	X	X	

BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	**MDL DOCKET NO. 2843**

PROOF OF SERVICE

In compliance with Rule 4.1(a) of the Rules of Procedure for the United States Judicial Panel on Multidistrict Litigation, I hereby certify that on April 6, 2018, I caused the foregoing document to be filed with the Clerk of the Court using the Judicial Panel on Multidistrict Litigation's CM/ECF system, which will serve notification of such filing to the email of all counsel of record in this action. I further certify that copies of the foregoing were served on all counsel (or unrepresented parties), and on the Clerk of the Court of each proposed transferor court, by U.S. First Class Mail, postage pre-paid, as follows:

Court Clerks

Susan Y. Soong, Clerk San Francisco Division United States District Court 450 Golden Gate Avenue, Box 36060 San Francisco, CA 94102	*Theresa Beiner and Brandon Haubert, on behalf of themselves and all others similarly situated v. Facebook, Inc., and Cambridge Analytica;* Case No. 3:18-CV-01953 *Howard O'Kelly, on behalf of himself and all others similarly situated v. Facebook, Inc., and Cambridge Analytica, LLC;* Case No. 3:18-CV-01915 *Lauren Price on behalf of herself and all others similarly situated v. Facebook, Inc. and Cambridge Analytica*; Case No. 3:18-CV-01732 *Jonathan D. Rubin, individually and on behalf of all those similarly situated v. Facebook, Inc., SCL Group, Global Science Research Ltd., and Cambridge Analytica LLC;* Case No. 3:18-cv-01852 *Debra Kooser and Margaret Frankiewicz v. Facebook, Inc., Cambridge Analytica, SCL Group, Ltd., Global Science Research, Ltd.*, Case No. 3:18-cv-02009 *Taylor Picha, individually and on behalf of all others similarly situated v. Facebook, Inc. and Cambridge Analytica*; Case No. 3:18-cv-02090
Thomas G. Bruton, Clerk Chicago Division Everett McKinley Dirksen United States Courthouse 219 South Dearborn Street Chicago, IL 60604	*Victor James Comforte, II and Brendan Michael Carr, Individually, and on behalf of all others similarly situated v. Cambridge Analytica, Facebook, Inc., Mark Zuckerberg, and John and Jane Does 1-100,* Case No. 1:18-CV-02120
Susan Y. Soong, Clerk Oakland Division United States District Court 1301 Clay Street, Suite 400S Oakland, CA 94612	*Ashley Gennock and Randy Nunez, and on behalf of all others similarly situated v. Facebook, Inc., and Cambridge Analytica;* Case No. 4:18-CV-01891 *Christina Labajo, individually and on behalf of herself and all others similarly situated v. Facebook, Inc. and Cambridge Analytica*; Case No. 4:18-cv-02093

Susan Y. Soong, Clerk San Francisco Division United States District Court 280 S. 1st Street San Jose, CA 95113	*Suzie Haslinger, individually and on behalf of all others similarly situated v. Facebook, Inc., Cambridge Analytica LLC, and DOES 1-100;* 4:18-cv-01984-YGR
Kiry Gray, Clerk Southern Division Central Division of California 411 West 4th Street, Room 1053 Santa Ana, CA 92701	*Jordan O'Hara, Brent Collins, and Olivia Johnston, individually and on behalf of all others similarly situated v. Facebook, Inc., a Delaware corporation; Cambridge Analytica, LLC, a Delaware limited liability company; Aleksandr Kogan, an individual, Stephen K. Bannon, an individual, and DOES 1-10, Inclusive*
David J. Bradley, Clerk Houston Division United States Courthouse 515 Rusk Avenue Houston, TX 77002	*Matthew Lodowski, individually and on behalf of all others similarly situated v. Facebook, Inc., Cambridge Analytica, Robert Leroy Mercer, and Aleksandr Kogan;* Case No. 4:18-CV-00907
William T. Walsh, Clerk Newark Division Martin Luther King Building & U.S. Courthouse 50 Walnut Street Newark, NJ 07101	*Jay Malskoff and Kenneth Irvine, individually and on behalf of all others v. Facebook, Inc., Cambridge Analytica, Cambridge Analytica (UK), Cambridge Analytica LLC, Robert Mercer, and Aleksandr Kogan;* Case No. 2:18-CV-04451
Clerk of Court Hugo L. Black United States Courthouse 1729 5th Avenue North Birmingham, AL 35203	*Jackie Williams, on behalf of herself and all others similarly situated v. Facebook, Inc. and Cambridge Analytica, LLC*, Case No. 2:18-CV-00535-RDP

Counsel / Parties

Michael W. Sobol Lieff Cabraser Heimann & Bernstein, LLP Embarcadero Center West 275 Battery Street, 29th Floor San Francisco, CA 94111-3339 Telephone: 415.956.1000 Fax: 415.956.1008 Email: msobol@lchb.com *Counsel to Plaintiff Theresa Beiner and Brandon Haubert*	Joseph Scott Davidson James C. Vlahakis Sulaiman Law Group, Ltd. 2500 S. Highland Avenue, Suite 200 Lombard, IL 60148 Telephone: 630.581.5456 Fax: 630-575.8188 Email: jvlahakis@sulaimanlaw.com *Counsel to Plaintiff Victor James Comforte, II and Brendan Michael Carr*

Todd David Carpenter
Carlson Lynch Sweet Kilpela & Carpenter LLP
1350 Columbia Street, Suite 603
San Diego, CA 92101
Telephone: 619.762.1900
Fax: 619.756.6991
Email: tcarpenter@carlsonlynch.com
Counsel to Plaintiff Ashley Gennock and Randy Nunez

Jason Scott Hartley
Stueve Siegel Hanson, LLP
550 West C Street
Suite 1750
San Diego, CA 92101
Telephone: 619.400.5822
Fax: 619.400.5832
Email: hartley@stuevesiegel.com
Counsel to Plaintiff Howard O'Kelly

Christopher Springer
Keller Rohrback, L.L.P.
801 Garden Street, Suite 301
Santa Barbara, CA 93101
Telephone: 805.456.1496
Fax: 805.456.1497
Email: cspringer@kellerrohrback.com
Counsel to Plaintiff Suzie Haslinger

John A. Yanchunis
Morgan and Morgan, P.A.
201 N. Franklin Street, 7th Floor
Tampa, FL 33602
Telephone: 813.223.5505
Fax: 813.223.5402
Email: jyanchunis@ForThePeople.com
Counsel to Plaintiff Lauren Price

Lynn Lincoln Sarko
Gretchen Freeman Cappio
Cari Campen Laufenberg
Keller Rohrback, L.L.P.
1201 Third Avenue, Suite 3200
Seattle, WA 98101
Telephone: 206.623.1900
Fax: 206.623.3384
Email: lsarko@kellerrohrback.com
Email: gcappio@kellerrohrback.com
Email: claufenberg@kellerrohrback.com
Counsel to Plaintiff Suzie Haslinger

Steven William Teppler
Abbott Law Group, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Telephone: 904.292.1111
Fax: 904.292.1220
Email: steppler@abbottlawpa.com
Counsel to Plaintiff Lauren Price

William Craft Hughes
Hughes Ellzey, LLP
Galleria Tower I
2700 Post Oak Blvd, Suite 1120
Houston, TX 77056
Telephone: 888.350.3931
Fax: 888.995.3335
Email: craft@hughesellzey.com
Counsel to Plaintiff Matthew Lodowski

Joshua Haakon Watson
Clayeo C. Arnold, A Professional Law Corporation
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.777.7777
Fax: 916.924.1829
Email: jwatson@justice4you.com
Counsel to Plaintiff Lauren Price

James E. Cecchi
Carella Byrne Cecchi Olstein Brody & Agnello, PC
5 Becker Farm Road
Roseland, NJ 07068
Telephone: 973.994.1700
Fax: 973.994.1744
Email: jcecchi@carellabyrne.com
Counsel to Plaintiffs Jay Malskoff and Kenneth Irvine

Nicholas A. Carlin
Phillips Erlewine Given & Carlin LLP
39 Mesa Street, Suite 201
The Presidio
San Francisco, CA 94129
Telephone: 415.398.0900
Fax: 415.398.0911
Email: nac@phillaw.com
Counsel to Plaintiff Jonathan D. Rubin

Helen I. Zeldes
Amy C. Johnsgard
Andrew J. Kubik
Ben Travis
Coast Law Group LLP
1140 S. Coast Highway 101
Encinitas, California 92024
Telephone: 760.942.8505
Fax: 760.942.8515
Email: helen@coastlaw.com
Email: amy@coastlaw.com
Email: andy@coastlaw.com
Email: ben@coastlaw.com
Counsel to Plaintiffs Jordan O'Hara, Brent Collins, and Olivia Johnston

Charles J. LaDuca
Cuneo Gilbert & LaDuca LLP
4725 Wisconsin Ave., NW, Suite 200
Washington, D.C. 20016
Telephone: 202.789.3960
Fax: 202.789.1813
Email: charlesl@cuneolaw.com
Counsel to Plaintiffs Jordan O'Hara, Brent Collins, and Olivia Johnston

Michael J. Flannery
Cuneo Gilbert & LaDuca LLP
7733 Forsyth Boulevard, Suite 1675
St. Louis, MO 63105
Telephone: 314.226.1015
Fax: 202.789.1813
Email: mflannery@cuneolaw.com
Counsel to Plaintiffs Jordan O'Hara, Brent Collins, and Olivia Johnston

Paul L. Hoffman
Aidan C. McGlaze
Schonbrun Seplow Harris & Hoffman LLP
11543 W. Olympic Blvd
Los Angeles, CA 90064
Telephone: 310.396.0731
Fax: 310.399.7040
Email: phoffman@sshhlaw.com
Email: amcglaze@sshhlaw.com
Counsel to Plaintiffs Jordan O'Hara, Brent Collins, and Olivia Johnston

Timothy G. Blood
Thomas J. O'Reardon II
Blood Hurst & O'Reardon, LLP
501 W. Broadway, Suite 1490
San Diego, CA 92101
Telephone: 619.339.1100
Fax: 619.338.1101
Email: tblood@bholaw.com
Email: toreardon@bholaw.com
Counsel to Plaintiffs Jordan O'Hara, Brent Collins, and Olivia Johnston

SCL Group
1-6 Yarmouth Place
Mayfair
London, W1S 4EL

Global Science Research Ltd.
6th Floor 49 Peter Street,
Manchester, England, M2 3NG

Orin Snyder
Gibson, Dunn & Crutcher, LLP
200 Park Avenue
New York, NY 10166
Tel: 212.351.2400
Fax: 212.351.6335
Email: osnyder@gibsondunn.com
Counsel for Mark Zuckerberg

Cambridge Analytica (UK) Ltd.
55 New Oxford Street
London WC1A 1BS

Robert Leroy Mercer
149 Harbor Rd.
Saint James, NY 11780

Aleksandr Kogan
University of Cambridge, Dept. of Psychology
Downing Street
Cambridge, UK CB2 3EB

The Corporation Trust Company
Corporation Trust Center
1209 Orange Street
Wilmington, DE 19801
Agent of Service of Process for Cambridge Analytica, LLC

Stephen K. Bannon
210 A Street, N.E.
Washington, DC 20002
Last Known Address

Joshua Haakon Watson
Clayeo C. Arnold, A Professional Law Corp.
865 Howe Avenue
Sacramento, CA 95825
Telephone: 916.777.7777
Fax: 916.924.1829
Email: jwatson@justice4you.com
Counsel for Debra Kooser and Margaret Frankiewicz

Luke Montgomery
Brad Ponder
Montgomery Ponder, LLC
2226 1st Avenue South, Suite 105
Birmingham, AL 35233
Telephone: 205.201.0303
Fax: 205.208.9443
Email: luke@montgomeryponder.com
Email: brad@montgomeryponder.com
Counsel for Jackie Williams

Jodi Westbrook Flowers
Ann Ritter
Fred Baker
Kimberly Barone Baden
Andrew Arnold
Annie Kouba
Motley Rice LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: 843.216.9000
Fax: 843.216.9450
Email: jflowers@motleyrice.com
Email: aritter@motleyrice.com
Email: fbaker@motleyrice.com
Email: kbaden@motleyrice.com
Email: aarnold@motleyrice.com
Email: akouba@motleyrice.com
Counsel for Taylor Picha

Will Lemkul
Morris Sullivan & Lemkul LLP
9915 Mira Mesa Boulevard, Suite 300
San Diego, CA 92131
Telephone: 858.566.7600
Fax: 858.566.6602
Email: lemkul@morrissullivanlaw.com
Counsel for Taylor Picha

Gordon M. Fauth, Jr.
Rosanne L. Mah
Finkelstein Thompson LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Telephone: 415.398.8700
Fax: 415.398.8704
Email: gfauth@finkelsteinthompson.com
Email: rmah@finkelsteinthompson.com
Counsel for Christina Labajo

Dated: April 6, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: /s/ *Orin Snyder*
Orin Snyder
200 Park Avenue
New York, N.Y. 10166
Tel: 212.351.2400
Fax: 212.351.6335
osnyder@gibsondunn.com

Joshua S. Lipshutz
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202.955.8217
Fax: 202.530.9614
jlipshutz@gibsondunn.com

Kristin A. Linsley
Brian M. Lutz
555 Mission Street
Suite 300
San Francisco, CA 94105
Tel: 415.393.8379
Fax: 415.374.8474
klinsley@gibsondunn.com
blutz@gibsondunn.com

Attorneys for Facebook, Inc.

BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	MDL DOCKET NO. 2843

NOTICE OF RELATED ACTIONS

Pursuant to Rule 6.2(d) of the Rules of Procedure of the Judicial Panel on Multidistrict Litigation ("the Panel"), Defendant Facebook, Inc. ("Facebook") hereby provides this notice informing the Panel of two related actions to In re Facebook, Inc., Consumer Privacy User Profile Litigation, MDL No. 2843:

1. *Christina Labajo v. Facebook, Inc., and Cambridge Analytica*, United States District Court for the Northern District of California (Oakland Division), 4:18-cv-02093 (filed Apr. 5, 2018)
2. *Taylor Picha v. Facebook, Inc. and Cambridge Analytica*, United States District Court for the Northern District of California (San Francisco Division), Case No. 3:18-cv-02090 (filed Apr. 5, 2018)

A schedule of actions is attached to this Notice. Copies of the docket sheets and complaints are attached as Exhibits A and B to this Notice. The complaints share common questions of fact and law and are premised on the same core issues as the other actions pending before the Panel, and are therefore "Related Actions" for purposes of these proceedings.

Dated: April 6, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Orin Snyder*

Orin Snyder
200 Park Avenue
New York, N.Y. 10166
Tel: 212.351.2400
Fax: 212.351.6335
osnyder@gibsondunn.com

Joshua S. Lipshutz
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202.955.8217
Fax: 202.530.9614
jlipshutz@gibsondunn.com

Kristin A. Linsley
Brian M. Lutz
555 Mission Street
Suite 300
San Francisco, CA 94105
Tel: 415.393.8379
Fax: 415.374.8474
klinsley@gibsondunn.com
blutz@gibsondunn.com

Attorneys for Facebook, Inc.

BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	MDL DOCKET NO. 2843

SCHEDULE OF ACTIONS (TO BE ADDED TO EXISTING SCHEDULE)

#	Case Name	District	Case No. / Filing Date	Assigned Judge
1	Christina Labajo v. Facebook, Inc. and Cambridge Analytica	Northern District of California (Oakland)	Case No.: 4:18-cv-02093 Filed: 04/05/2018	Magistrate Judge Kandis A. Westmore
2	Taylor Picha v. Facebook, Inc. and Cambridge Analytica	Northern District of California (San Francisco)	Case No.: 3:18-cv-02090 Filed: 04/05/2018	Magistrate Judge Sallie Kim

Dated: April 6, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: /s/ *Orin Snyder*

Orin Snyder
200 Park Avenue
New York, N.Y. 10166
Tel: 212.351.2400
Fax: 212.351.6335
osnyder@gibsondunn.com

Joshua S. Lipshutz
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202.955.8217
Fax: 202.530.9614
jlipshutz@gibsondunn.com

Kristin A. Linsley
Brian M. Lutz
555 Mission Street
Suite 300
San Francisco, CA 94105
Tel: 415.393.8379
Fax: 415.374.8474
klinsley@gibsondunn.com
blutz@gibsondunn.com

Attorneys for Facebook, Inc.

BEFORE THE
UNITED STATES JUDICIAL PANEL ON
MULTIDISTRICT LITIGATION

IN RE: FACEBOOK, INC., CONSUMER PRIVACY USER PROFILE LITIGATION	MDL DOCKET NO. 2843

PROOF OF SERVICE

In compliance with Rule 4.1(a) of the Rules of Procedure for the United States Judicial Panel on Multidistrict Litigation, I hereby certify that on April 6, 2018, I caused the foregoing documents to be filed with the Clerk of the Court using the Judicial Panel on Multidistrict Litigation's CM/ECF system, which will serve notification of such filing to the email of all counsel of record in this action. I further certify that copies of the foregoing were served on all counsel (or unrepresented parties), and on the Clerk of the Court of each proposed transferor court, by U.S. First Class Mail, postage pre-paid, as follows:

Court Clerks

Susan Y. Soong, Clerk
Ronald V. Dellums Federal Building
& United States Courthouse
Oakland Division
1301 Clay Street
Oakland, CA 94612

Christina Labajo, individually and on behalf of herself and all others similarly situated v. Facebook, Inc. and Cambridge Analytica; Case No. 4:18-cv-02093

Susan Y. Soong, Clerk
San Francisco Division
United States District Court
450 Golden Gate Avenue, Box 36060
San Francisco, CA 94102

Taylor Picha, individually and on behalf of all others similarly situated v. Facebook, Inc. and Cambridge Analytica; Case No. 3:18-cv-02090

Counsel / Parties

Jodi Westbrook Flowers
Ann Ritter
Fred Baker
Kimberly Barone Baden
Andrew Arnold
Annie Kouba
Motley Rice LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: jflowers@motleyrice.com
Email: aritter@motleyrice.com
Email: fbaker@motleyrice.com
Email: kbaden@motleyrice.com
Email: aarnold@motleyrice.com
Email: akouba@motleyrice.com
Counsel for Taylor Picha

Will Lemkul
Morris Sullivan & Lemkul LLP
9915 Mira Mesa Boulevard, Suite 300
San Diego, CA 92131
Telephone: (858) 566-7600
Facsimile: (858) 566-6602
Email: lemkul@morrissullivanlaw.com
Counsel for Taylor Picha

Gordon M. Fauth, Jr.
Rosanne L. Mah
Finkelstein Thompson LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Telephone: (415) 398-8700
Facsimile: (415) 398-8704
Email: gfauth@finkelsteinthompson.com
Email: rmah@finkelsteinthompson.com
Counsel for Christina Labajo

The Corporation Trust Company
Corporation Trust Center
1209 Orange Street
Wilmington, DE 19801
Agent of Service of Process for Cambridge Analytica, LLC

Dated: April 6, 2018

Respectfully submitted,

GIBSON, DUNN & CRUTCHER LLP

By: */s/ Orin Snyder*

Orin Snyder
200 Park Avenue
New York, N.Y. 10166
Tel: 212.351.2400
Fax: 212.351.6335
osnyder@gibsondunn.com

Joshua S. Lipshutz
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Tel: 202.955.8217
Fax: 202.530.9614
jlipshutz@gibsondunn.com

Kristin A. Linsley
Brian M. Lutz
555 Mission Street
Suite 300
San Francisco, CA 94105
Tel: 415.393.8379
Fax: 415.374.8474
klinsley@gibsondunn.com
blutz@gibsondunn.com

Attorneys for Facebook, Inc.

EXHIBIT A

ADRMOP

U.S. District Court
California Northern District (Oakland)
CIVIL DOCKET FOR CASE #: 4:18-cv-02093-KAW

Labajo v. Facebook Inc. et al
Assigned to: Magistrate Judge Kandis A. Westmore
Cause: 28:1331 Fed. Question

Date Filed: 04/05/2018
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: Federal Question

Plaintiff

Christina Labajo
an Individual, on behalf of herself and all others similarly situated

represented by **Rosanne L. Mah**
Finkelstein Thompson
100 Pine Street
Suite 1250
San Francisco, CA 94111
(415) 398-8700
Fax: (415) 398-8704
Email: rlm@classlitigation.com
ATTORNEY TO BE NOTICED

Gordon M. Fauth , Jr.
Litigation Law Group
1801 Clement Av
Suite 101
Alameda, CA 94501
(510) 238-9610
Fax: (510) 337-1431
Email: gmf@classlitigation.com
ATTORNEY TO BE NOTICED

V.

Defendant

Facebook Inc.

Defendant

Cambridge Analytica

Date Filed	#	Docket Text
04/05/2018	1	COMPLAINT against All Defendants (Filing fee $ 400, receipt number 0971-12251479.). Filed byChristina Labajo. (Attachments: # 1 Civil Cover Sheet Civil Cover Sheet)(Fauth, Gordon) (Filed on 4/5/2018) (Entered: 04/05/2018)

04/05/2018	2	Proposed Summons. (Fauth, Gordon) (Filed on 4/5/2018) (Entered: 04/05/2018)
04/05/2018	3	Proposed Summons. (Fauth, Gordon) (Filed on 4/5/2018) (Entered: 04/05/2018)
04/05/2018	4	Case assigned to Magistrate Judge Kandis A. Westmore. Counsel for plaintiff or the removing party is responsible for serving the Complaint or Notice of Removal, Summons and the assigned judge's standing orders and all other new case documents upon the opposing parties. For information, visit *E-Filing A New Civil Case* at http://cand.uscourts.gov/ecf/caseopening. Standing orders can be downloaded from the court's web page at www.cand.uscourts.gov/judges. Upon receipt, the summons will be issued and returned electronically. Counsel is required to send chambers a copy of the initiating documents pursuant to L.R. 5-1(e)(7). A scheduling order will be sent by Notice of Electronic Filing (NEF) within two business days. Consent/Declination due by 4/19/2018. (bwS, COURT STAFF) (Filed on 4/5/2018) (Entered: 04/06/2018)
04/06/2018	5	**Initial Case Management Scheduling Order with ADR Deadlines: Case Management Statement due by 7/3/2018. Initial Case Management Conference set for 7/10/2018 01:30 PM. (cp, COURT STAFF) (Filed on 4/6/2018) (Entered: 04/06/2018)**
04/06/2018	6	Summons Issued as to Cambridge Analytica, Facebook Inc.. (Attachments: # 1 Cambridge Analytica)(cp, COURT STAFF) (Filed on 4/6/2018) (Entered: 04/06/2018)

PACER Service Center			
Transaction Receipt			
04/06/2018 12:15:26			
PACER Login:	gd0021DA:2553423:4036719	**Client Code:**	30993-00083
Description:	Docket Report	**Search Criteria:**	4:18-cv-02093-KAW
Billable Pages:	1	**Cost:**	0.10

Gordon M. Fauth, Jr. (SBN 190280)
gfauth@finkelsteinthompson.com
Of Counsel
Rosanne L. Mah (Cal. Bar No. 242628)
rmah@finkelsteinthompson.com
Of Counsel
FINKELSTEIN THOMPSON LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Direct Telephone: (510) 238-9610
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Attorneys for Individual and Representative
Plaintiff Christina Labajo

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

CHRISTINA LABAJO, an Individual, on behalf of herself and all others similarly situated, Plaintiff, vs. FACEBOOK, INC. and CAMBRIDGE ANALYTICA, Defendants.	Case No. **CLASS ACTION COMPLAINT FOR DAMAGES AND EQUITABLE RELIEF** **JURY TRIAL DEMANDED**

Plaintiff Christina Labajo, individually and on behalf of all others similarly situated, by and through her undersigned counsel, for her complaint brings this class action for damages and equitable relief against Defendants Facebook, Inc. and Cambridge Analytica. Plaintiff alleges the following upon information and belief based on the investigation of counsel, except as to those allegations that specifically pertain to Plaintiff, which are alleged upon personal knowledge:

NATURE OF THE ACTION

1. This is a civil action brought by Plaintiff Christina Labajo ("Labajo" or "Plaintiff") on behalf of herself and all others similarly situated against Defendants Facebook, Inc. ("Facebook") and Cambridge Analytica ("Cambridge Analytica") (collectively "Defendants"). In this action, Plaintiff alleges that in June-August 2014 Facebook allowed a massive data breach in which the sensitive personal information of Plaintiff and 87 million Facebook users (including 71 million Americans) was misappropriated by Cambridge Analytica and other entities and used for unauthorized purposes, including attempts to influence the 2016 United States presidential election (the "Data Breach" or "2014 Data Breach"). Plaintiff further alleges that for years, Facebook allowed hackers to exploit known vulnerabilities in its network to "scrape" data from users' profiles, violating their privacy and placing them at risk for identity theft.

2. Facebook is a popular Internet social networking service located at www.facebook.com. Facebook has more than two billion users worldwide.[1] Facebook allows registered users to utilize their Facebook accounts and timeline pages to share information with and communicate with friends, family, and colleagues. Facebook users create customized profiles and pages containing highly personal information, including their name, home address, email address, telephone numbers, birthdate, gender, interests, relationships, photographs and videos, "likes" and other information (hereafter, "Personal Information"). Facebook users can share this Personal Information and exchange messages with other users.

3. Cambridge Analytica is a political consulting firm engaged in data mining, data analysis and consulting on behalf of political clients, in an effort to influence the outcomes of elections.[2] Notably, it was hired to provide data and analytical services, first to the Ted Cruz primary campaign and then to the 2016 presidential campaign of Donald Trump. Among other things, Cambridge Analytica used Facebook users' personal data to build "psychographic" profiles so that these potential voters could be targeted with tailored advertising messages

---

[1] *See* https://en.wikipedia.org/wiki/Facebook (last visited March 25, 2018).

[2] *See* https://en.wikipedia.org/wiki/Cambridge Analytica_Analytica#cite_note-ca-9 (last visited March 25, 2018).

designed to influence their voting.

4. Facebook falsely promised its users their Personal Information would be protected and not shared with others except as they authorized. In fact, Facebook knew its security was inadequate to protect users' data, and that its default settings and available tools coupled with security vulnerabilities made it easy for hackers to gain access to users' information. Also, Facebook had a policy of selling user data to third parties and even implemented APIs to allow third-party apps to "harvest" user information for their own purposes.

5. On March 17, 2018, the *New York Times* and *The Guardian* reported that Cambridge Analytica had gained access to the "harvested" Personal Information of more than 50 million Facebook users, which had been taken in a massive data breach in 2014. The stolen information was, among other things, used to construct psychological profiles of the Facebook users, so that they could be targeted with advertising in an attempt to influence their voting in the 2016 presidential election.

6. After initially threatening legal action in an attempt to suppress the news reports, once the news was published, Facebook was forced to concede the data breach had taken place. On April 4, 2018, Facebook admitted that the data breach was even larger than reported, and that as many as 87 million Facebook users, the vast majority in the United States, had their Personal Information stolen.

7. In a further revelation on April 4, 2018, Facebook disclosed that, in addition to the Cambridge Analytica data breach, "malicious actors" had for years been using search tools on its platform to "scrape" identities and other profile information on "most" of its 2 billion users worldwide.

8. The Cambridge Analytica data theft occurred June through August 2014. The data "harvesting" was done by recruiting a Cambridge University researcher to develop an app called ThisIsYourDigitalLife, with financial backing from Cambridge Analytica, which was used to access Facebook users' Personal Information. Misleadingly billed as a "personality quiz" given as part of a research project, participants were promised a personality assessment. Some 270,000 Facebook users were tricked into using the app, and Facebook allowed the app to harvest not only their Personal Information but also the Personal Information of each of those

user's circles of Facebook "friends." Because of this multiplying effect, the Data Breach resulted in the theft of the Personal Information of 87 million Facebook users, 71 million of them in the United States.

9. Even though Facebook knew of the 2014 Data Breach and its extent in 2015 and perhaps earlier, Facebook failed to disclose the breach to the owners of the stolen Personal Information or to the public. Facebook acknowledged the breach and its extent only after the news media published reports of the data breach in March 2018. On March 21, 2018, Facebook CEO Mark Zuckberg conceded the breach had happened and admitted it constituted a "breach of trust between Facebook and the people who share their data with us and expect us to protect it."[3]

10. Facebook has failed to protect personal and private information entrusted to it by Plaintiff and other consumers, and has allowed this highly sensitive information to be "harvested," misappropriated and misused. Because of the 2014 Data Breach, the privacy of Plaintiff and millions of Facebook users has been invaded, and their Personal Information is in the hands of Cambridge Analytica and unknown others and, according to experts, is likely to be proliferating out on the "dark web." Because of the data "scraping" that Facebook has allowed to happen for years, personal and private information of virtually all Facebook users is now in the hands of unknown hackers. These Facebook users have not only had their privacy invaded, they now must live under the continual threat of their personal and private information being used for identity theft and other nefarious purposes.

11. Plaintiff and other Facebook users in California and across the United States have suffered harm because of Facebook's failure to take adequate security measures to protect their personal and private information and because Facebook allowed the misappropriation of their sensitive data. Facebook's failure to disclose to Plaintiff and other Facebook users that it did not adequately protect information entrusted to it, its malfeasance in allowing their data to be taken, and its failure to disclose the occurrence of the data theft and the scope of the theft until the news media left it little choice, are made the more egregious by the fact that Facebook in 2011 entered into a consent decree settlement of an FTC action in which Facebook was accused of allowing

[3] *See* https://www.facebook.com/zuck/posts/10104712037900071 (last visited March 25, 2018).

user data to fall into the wrong hands. As part of the settlement, Facebook promised to take effective measures to guard against user information being compromised. Nonetheless, Facebook willfully chose not to take the measures that it knew were necessary to protect the sensitive user data in its keeping, and instead allowed hackers and third-party apps to access the personal and private information of users; and as a result has caused harm to Plaintiff and Class members.

12. Defendants' actions and omissions violate laws including the Security Breach Notification Law, Cal. Civil Code § 1798.82; the Customer Records Act, Cal. Civ. Code § 1798.81.5; the Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*; the Electronic Communications Privacy Act, 18 U.S.C §§ 2511 *et seq;* the Stored Communication Act, 18 U.S.C § 2701, *et seq.* and constitute negligence, misappropriation, and unjust enrichment.

13. Accordingly, Plaintiff brings this case on behalf of herself and other similarly situated persons and seeks damages including compensatory and statutory damages, punitive damages, and equitable relief, declaratory relief, and attorney fees and costs.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because claims under federal law are pleaded, and pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million, exclusive of interests and costs; the number of members of each of the proposed Classes exceeds 100; and many class members are citizens of states different from the states of which Defendants are citizens.

15. This Court has personal jurisdiction over the Defendants because they conduct substantial business in the State of California and in this Judicial District and/or the conduct complained of occurred in and/or emanated from this State and Judicial District.

16. Venue is proper in this Judicial District because Defendants conduct substantial business in this Judicial District and/or the conduct complained of occurred in or emanated from this District.

INTRADISTRICT ASSIGNMENT

17. Venue is proper in this Judicial District and the San Jose division thereof pursuant to 28 U.S.C. section 1391 subsections (b) and (c), and Civil L.R. 3-2 subsections (c) and (d). Defendants transact business in this division and County and/or a substantial part of the events

giving rise to the claims at issue in the litigation arose in this division and County.

PARTIES

Plaintiff

18. Plaintiff Christina Labajo is and has at all relevant times been a resident of California. Plaintiff has held a Facebook account since 2009.

19. Plaintiff's Personal Information was misappropriated by Cambridge Analytica in the Data Breach complained of herein, and as a result Plaintiff was subjected to unwanted and misleading, targeted political ads designed to brainwash and improperly influence her vote during the 2016 Presidential election. Plaintiff also had her profile information taken by unknown entities in the "scraping" revealed by Facebook on April 4, 2018. Plaintiff was injured because her personal information was collected and misused in violation of Facebook's promises of protection of her privacy. Plaintiff was also injured because her personal information stored on Facebook had commercial value, and that value was misappropriated and employed for the profit of Defendants.

20. Plaintiff did not give consent to the sharing of her Personal Information with Cambridge Analytica or unknown hackers.

Defendants

21. Defendant Facebook, Inc. is a Delaware corporation with headquarters in Menlo Park, California. Its primary business consists of providing online social networking service to its users and selling advertising to businesses who want to reach its users. Facebook states that its mission is to "[g]ive people the power to build community and bring the world closer together." Founded on February 4, 2004, Facebook has grown to have more than two billion users worldwide. It employs over 25,000 employees. It has over 50 offices and 12 data centers throughout the world.

22. Facebook's revenues come from advertising directed to its users and from providing user information to third party entities. In 2017, Facebook's revenues were $40.65 billion. Traded publicly on Nasdaq (Symbol: FB), Facebook has a market cap of $464 billion.

23. Defendant Cambridge Analytica is a London-based privately held company with offices in New York, Washington, D.C., and London. Cambridge Analytica is a subsidiary of

Strategic Communications Laboratories ("SCL"), a British company whose stated purpose is to "create behavior change through research, data analytics, and strategy for both domestic and international government clients." Cambridge Analytica was formed in 2013, with funding from hedge-fund billionaire Robert Mercer, and co-founder alt-right publisher and strategist Steve Bannon as vice-president, specifically to use SCL technology to influence the American political process. Cambridge Analytica has performed voter data analysis services for numerous political campaigns in the United States, including the 2016 presidential campaign of Donald Trump.

24. Cambridge Analytica uses data mining and analysis to formulate "strategic communications" aimed at voters in an effort to influence the electoral process. Alexander Nix, Cambridge Analytica's CEO, has admitted the company uses tricks to influence elections.[4] "This January, in undercover footage filmed by Channel 4 News in Britain and viewed by The Times, he boasted of employing front companies and former spies on behalf of political clients around the world, and even suggested ways to entrap politicians in compromising situations."[5]

TOLLING OF STATUTES OF LIMITATION

25. Plaintiff and Class members did not, and even with diligent effort could not have, learned of the 2014 Data Breach and misuse of their Personal Information complained of herein until it was reported in the news media on March 17, 2018, and with respect to the "scraping" of profile information by as-yet-unknown hackers, until Facebook's revelations on April 4, 2018. Accordingly, all applicable statutes of limitation are tolled and do not begin to run until March 17 and April 4, 2018.

SUBSTANTIVE ALLEGATIONS COMMON TO ALL CAUSES OF ACTION

The Facebook Social Media and Networking Site

26. Facebook operates a popular social media and networking site, located at www.facebook.com. Facebook was founded in 2004 by CEO Mark Zuckerberg, then an

---

[4] *See* https://www.theguardian.com/uk-news/2018/mar/19/Cambridge Analytica-analytica-execs-boast-dirty-tricks-honey-traps-elections (last visited March 25, 2018).

[5] *How Trump Consultants Exploited the Facebook Data of Millions,* https://www.nytimes.com/2018/03/17/us/politics/Cambridge Analytica-analytica-trump-campaign.html (last visited 3/30/18).

undergraduate student at Harvard University, as a social networking service for Harvard college students. The founders, essentially Zuckerberg and his roommates, called the online service "Facebook" after the paper book directory colleges gave to their students. Facebook first expanded to other elite colleges, then quickly expanded beyond the student world, growing into the world's premier social networking site. Facebook now has "2.13 billion monthly active users as of December 31, 2017."[6]

27. Users establish accounts on Facebook and set up a Profile containing personal information about themselves. Facebook gives each user a Timeline or user page that other Facebook users can visit. The Timeline is a reverse-chronology blog:

> "Timeline is a section of a Facebook user's account that replaces the Profile and Wall pages, and merges them together. It shows the story of your life, as you choose to tell it or as Facebook has recorded it, in a visual, scrolling, reverse-chronologically ordered timeline. It's a cross between visual blog and online scrapbook."[7]

28. On the user's Timeline page, certain profile information appears, and users also post additional personal information and news, photos, videos and other Personal Information. Users typically maintain their pages as a type of constantly updated blog. Facebook facilitates messaging between users and offers participation in online games as well as furnishing a variety of other services to users.

29. Facebook members can generally specify whether personal information they give Facebook or information they post on their Timeline page can be seen by all Facebook users, only Facebook users they have accepted as "Friends," Friends with certain exceptions, or only selected Friends. Depending on settings, users' news postings may also appear automatically on all of their Friends' pages. Users can also post on Friend's pages, subject to deletion by the Friend. Users send "Friend Requests" to other users, which may be accepted or rejected. Facebook advises:

---

[6] *See* https://newsroom.fb.com/company-info/ (last visited March 26, 2018).

[7] *12 Things You Should Know About Facebook Timeline, at* https://www.pcmag.com/article2/0,2817,2393464,00.asp (last visited 3/30/18).

> "You should send friend requests to friends, family and other people on Facebook you know and trust. You can add a friend by searching for them and sending them a friend request. If they accept, you automatically follow that person, and they automatically follow you — which means that you may see each other's posts in News Feed."

30. A Facebook user will typically have a wide circle of Friends, changing constantly as new Friends are made or old Friends unfriended. A Facebook visitor to a user's page may click to "like" or select other emoticons to indicate their feelings concerning the user's postings and content. The acrimony and perceived snubs involved in the interaction and Friending/Unfriending process has contributed significantly to the anxiety levels of many Facebook users, particularly the younger ones.

31. Anyone who says they are at least 13 years is allowed to open a Facebook account, except where prohibited by local laws.

Facebook is Big Business

32. Facebook's service is free for consumer users. However, Facebook generates enormous revenues. Facebook derives its revenues from advertisers who pay Facebook for popup ads targeted to its users based on their Profile information and from third party entities that pay for Facebook users' data. As Facebook tells advertisers, "With our powerful audience selection tools, you can target the people who are right for your business. Using what you know about your customers—like demographics, interests and behaviors—you can connect with people similar to them."[8]

33. Advertising is a lucrative business for Facebook. In 2017, Facebook's revenues from advertising were $ $40.65 billion, up from $26.89 billion in 2016. Most of Facebook's revenue comes from popup or banner ads. However, Facebook also derives revenue from selling third parties "firehose" bulk access to Facebook users' data.[9]

Consumers Entrust Facebook With Their Personal Information

34. Users are encouraged to provide profile information and post personal

---

[8] *See* https://www.facebook.com/business/products/ads/ad-targeting (last visited 3/29/2018).

[9] *See* Wikipedia *at* https://en.wikipedia.org/wiki/Facebook (lasted visited 3/29/2018).

information about themselves, including their name, home address, email address, telephone numbers, birthdate, gender, interests, relationships, photographs and videos, activities, "likes" and other information. In addition to viewing posted information, users may use their Facebook account to send messages and communicate with each other. Facebook allows people to "stay connected" with friends, family, and colleagues to "discover what's going on in the world," and to share information and "express what matters to them."[10]

35. Users provide Facebook with their profile and Personal Information, believing it will be protected from unauthorized disclosure and misuse. Facebook promises to give members the ability to control and manage their privacy. "You have control over who sees what you share on Facebook…You're In Charge…so you can confidently share your moments."[11]

36. Facebook assures its users that their profile and Personal Information is protected from hackers and misappropriation. Facebook states it has "top-rate security measures in place to help protect you and your data when you use Facebook."[12] Facebook assures its users that "[w]hen it comes to your personal information, we don't share it without your permission."[13]

Facebook's Inadequate Security Measures and Willful and Negligent Practices

37. Contrary to its assurances to Facebook users that their sensitive information was protected and safe, in fact, Facebook willfully, recklessly and negligently made its users' data including their profile and Personal Information accessible to third-party entities, for its own profit and/or through its reckless practices and policies.

38. In addition to allowing advertisers to target Facebook users on their Facebook pages with directed advertising based on users' profile and demographic information, Facebook also derives revenues from providing third party entities with bulk access to Facebook users' data. To facilitate such data acquisition, in 2010, Facebook launched its Open Graph API, to

---

[10] *See* https://investor.fb.com/resources/default.aspx (last visited March 26, 2018).

[11] *See* https://www.facebook.com/about/basics (last visited March 26, 2018).

[12] *See* https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected (last visited March 26, 2018)

[13] *See* https://www.facebook.com/about/basics/stay-safe-and-secure/how-youre-protected#4 (last visited March 26, 2018).

allow outside app developers to access user data. Facebook allows third-party entities to use apps to gain access to the Personal Information of users who have ostensibly consented to the app's access. In some cases, these third-party app developers may even gain access to a user's private messages.

39. At the same time that it shared user date with other entities, Facebook deliberately made it difficult for users to understand that they were sharing personal information with outside entities, or to understand what information would be shared. This was particularly true at the time of the 2014 data breach. For example, in or around 2012, Facebook changed the options on the permissions page for games from "Allow" and "Don't Allow" to simply "Play Game." "Play Game" did not communicate clearly to users that, by using a game app, they were opting into sharing data. Facebook also hid its explanation of what it considered "basic information" that would be routinely shared underneath a small "?" symbol that users needed to hover over to read.

40. By default, users' accounts settings failed to provide even the protection that was available to Facebook users, and Facebook failed to notify users of the dangers and adequately explain the options available to protect their data.

41. Worse, at the time of the 2014 Data Breach complained of herein, Facebook allowed third-party entities to use apps to harvest the Personal Information not just of users who had purportedly (according to Facebook) "consented" to the app's intrusion but also the Personal Information of other Facebook users who were those users' Friends. Since Facebook users each typically have a wide circle of Friends, this policy greatly multiplied the number of users whose Personal Information Facebook made available for harvesting by third-party apps.

42. Also, as now revealed, Facebook has for years allowed hackers to gain access to user data utilizing known vulnerabilities in the Facebook network, including using Facebook's own search tools to access user data. By allowing this "scraping" of user data and profile information, Facebook has facilitated the invasion of the privacy of virtually all its users, placing them at risk for identity theft.

ThisIsYourDigitalLife App Used to Steal Personal Information of 87 Million Facebook Users

Used By Cambridge Analytica in Attempt to Influence 2016 Presidential Election

43. On March 17, 2018, the *New York Times* and *The Guardian* reported that Cambridge Analytica had gained possession of the Personal Information of more than 50 million Facebook users in the United States that it acquired as the result of a massive 2014 data breach in which the Profile information of these users had been downloaded from Facebook ("Data Breach" or "2014 Data Breach"). On April 4, 2018, Facebook revealed that as many as 87 million users, including 71 million Americans, had their Personal Information taken in this Data Breach.

44. As reported in the *New York Time* and *The Guardian*, the massive Data Breach took place in 2014. Cambridge Analytica used the purloined Personal Information -- which represented nearly a third of potential U.S. voters -- to construct psychological profiles of those Facebook users which it then used to formulate strategies and direct tailored advertising on behalf of dozens of political campaign clients, including the Ted Cruz presidential campaign.

45. In 2016, after Senator Cruz dropped out of the race, the Donald Trump presidential campaign hired Cambridge Analytica to provide analytical and other services; and Cambridge Analytica used the stolen Personal Information and the "psychographic" profiles it created from the data to direct political ads and messages to Facebook users in an attempt to sway swing voters and influence the presidential election.

46. As explained by Christopher Wylie, a former Cambridge Analytica employee turned whistleblower, "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on."[14]

47. The March 17, 2018 reports on the Data Breach were in large part made possible by information provided to *The Guardian* by Christopher Wylie who, while employed by

[14] See https://www.theguardian.com/news/2018/mar/17/Cambridge Analytica-analytica-facebook-influence-us-election (last visited March 26, 2018).

Cambridge Analytica, had been intimately involved in the scheme to acquire and use Facebook user data:

> Aged 24, while studying for a PhD in fashion trend forecasting, he came up with a plan to harvest the Facebook profiles of millions of people in the US, and to use their private and personal information to create sophisticated psychological and political profiles. And then target them with political ads designed to work on their particular psychological makeup.[15]

48. As a result of having their Personal Information taken in the Data Breach, Plaintiff and members of the Classes were subjected to unwanted, false and misleading, targeted political ads during the 2016 Presidential election while using Facebook.

How the 2014 Data Breach Happened

49. In the June-August 2014 Data Breach, the Personal Information of Plaintiff and 87 million Facebook users (71 million American Facebook users) was taken using an app created for that purpose, designed to exploit Facebook's reckless policies that allowed data harvesting by third-party entities' apps.

50. In or around 2013, Cambridge Analytica and/or its parent SCL approached researchers at Cambridge University's Psychometrics Centre, who had pioneered work on large-scale data analysis, who had used Facebook data concerning users' personality traits to predict "behaviour from online footprints."[16] Cambridge Analytica was interested in acquiring the data and the software used to harvest the Facebook user data.

51. While the Centre and its key researchers apparently refused its overtures, Cambridge Analytica was able to enlist the aid of Aleksandr Kogan ("Kogan"), one of the researchers. Kogan created an app called "ThisIsYourDigitalLife," with Cambridge Analytica covering the more than $800,000 development costs of the app. The app purported to be a

---

[15] *'I Made Steve Bannon's Psychological Warfare Tool': Meet The Data War Whistleblower,* The Guardian (March 18, 2018) https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (last visited 4/4/18).

[16] *Cambridge Analytica Academic's Work Upset University Colleagues,* The Guardian, Mar. 24, 2108, *at* https://www.theguardian.com/education/2018/mar/24/cambridge-analytica-academics-work-upset-university-colleagues (last visited 3/30/18).

personality quiz and was falsely billed as a "research app used by psychologists," but its real purpose was to harvest the Personal Information of Facebook users.

52. In 2014, after the ThisIsYourDigitalLife app was successfully developed, Defendants advertised the app to Facebook users, and approximately 270,000 Facebook users participated in the "quiz." As allowed by Facebook, the app used Facebook's API to access and acquire the Personal Information of those "participating" persons and also the Personal Information of some 87 million other Facebook users within their circles of Friends.[17]

> The data analytics firm that worked with Donald Trump's election team and the winning Brexit campaign harvested millions of Facebook profiles of US voters, in one of the tech giant's biggest ever data breaches, and used them to build a powerful software program to predict and influence choices at the ballot box.
>
> A whistleblower has revealed to the Observer how Cambridge Analytica – a company owned by the hedge fund billionaire Robert Mercer, and headed at the time by Trump's key adviser Steve Bannon – used personal information taken without authorization in early 2014 to build a system that could profile individual US voters, in order to target them with personalized political advertisements.
>
> Christopher Wylie, who worked with a Cambridge Analytica University academic to obtain the data, told the Observer: "We exploited Facebook to harvest millions of people's profiles. And built models to exploit what we knew about them and target their inner demons. That was the basis the entire company was built on."
>
> --Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 Million Facebook Profiles Harvested For Cambridge Analytica In Major Data Breach,* The Guardian (March 17, 2018).

53. In their March 17, 2018 exposè, the *New York Times* and *The Guardian* reported that Cambridge Analytica was still in possession of the Personal Information that it had illegally acquired from millions of Facebook users without their permission.

Facebook Had Been Warned of such Data Breaches

Violation of 2011 FTC Consent Decree

54. At the time of the breach, Facebook was on notice of the dangers of such

---

[17] *See* https://www.facebook.com/zuck/posts/10104712037900071 (last visited March 26, 2018).

breaches. In 2011, Facebook entered into a consent decree to settle an FTC case, pursuant to which Facebook was not to share users' personal information with other entities.[18] This was the result of charges brought by the FTC, charging that Facebook had engaged in "unfair and deceptive practices" by making public the private data of its users and by inappropriately sharing user data with advertisers and outside application developers.[19]

55. Pursuant to the consent decree settling the 2011 FTC action, Facebook was to establish and maintain "a comprehensive privacy program" to address privacy risks and protect people's information.[20] The consent decree also required Facebook not to misrepresent to users the extent to which their data would be used. *Id.*

56. On March 20, 2018, following news of the massive 2014 data breach, the FTC launched an investigation into whether Facebook violated the 2011 consent decree. If found guilty, Facebook could face fines up to $40,000 per violation per day, resulting in $2 trillion in fines.[21]

57. Facebook was also criticized for a 2012 study involving a News Feed experiment designed to influence Facebook users' emotions. Nearly 700,000 users were subjected to this study without their explicit consent. This spurred widespread outrage privacy concerns by Facebook users, following which Facebook reportedly strengthened protections for users and added the "research policy" clause that was exploited in the ThisIsYourDigitalLife breach.

Facebook's Knowledge of the Breach and Attempts to Conceal the Breach

58. Facebook learned of the breach soon after it occurred. In or around 2015, Facebook learned that Kogan had shared data harvested using the ThisIsYourDigitalLife app with Cambridge Analytica. Yet, Facebook failed to inform its users whose Personal Information had been misappropriated and failed to inform the public. Instead, Facebook attempted to

---

[18] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (last visited 3/30/18).

[19] https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf (FTC complaint against Facebook) (last visited 3/30/18).

[20] https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf (last visited 3/30/18).

[21] *See* https://www.wired.com/story/ftc-facebook-data-privacy-investigation/ (last visted April 2, 2018).

conceal the breach.

59. According to Mark Zuckerberg's later admissions, since it was against Facebook's policies for app developers to share data, in 2015 Facebook demanded that Kogan and Cambridge Analytica certify that they had deleted all improperly acquired data. Facebook says Kogan and Cambridge Analytica provided the certifications; however, Facebook did nothing to verify that the purloined Personal Information had been deleted, which, in fact, did not take place.

60. On or around April 30, 2015, in response to the breach, Facebook updated its platform to provide approved third party apps with less data, particularly about users' friends, and to offer users more control over what information would be shared with third-party apps.

61. Facebook, however, made no effort to inform its users on a timely basis that their Personal Information was being, or had been, improperly harvested and misused.

62. When *The Guardian* approached Facebook for comments as it was investigating the story, Facebook threatened *The Guardian* with legal action if it published news of the breach. Facebook now acknowledges the threat was "not our wisest move."[22]

63. On March 19, 2018, in response to the *New York Time* and *The Guardian* stories revealing the Data Breach, which were based in part on information provided by former Cambridge Analytica employee and whistleblower Christopher Wylie, Facebook suspended Mr. Wylie's Facebook account.

64. Because of Facebook's concealment of the breach and its scope, the March 17, 2018 news reports by the *New York Times* and *The Guardian* was the first notice Plaintiff and other consumers received that their Personal Information was improperly harvested and misused.

Facebook's Belated Acknowledgement That It Betrayed Users' Trust

65. Following the March 17, 2018 media reports, Facebook finally admitted the data breach and its extent. On March 21, 2018, Facebook's CEO, Mark Zuckerberg, admitted that

---

[22] *Facebook News Head Says Threatening To Sue The Guardian Over Data Leak Was 'Not Our Wisest Move'*, CNBC, at https://www.cnbc.com/2018/03/22/facebook-says-threatening-to-sue-the-guardian-was-not-our-wisest-move.html (last visited 3/30/18).

"[Facebook] made mistakes" and said it was "a breach of trust between Kogan, Cambridge Analytica and Facebook. But it was also a breach of trust between Facebook and the people who share their data with us and expect us to protect it. We need to fix that."[23] Mark Zuckerberg also admitted it had been "a mistake" to rely on Kogan and Cambridge Analytica's certifications that they had destroyed the improperly acquired data.

66. According to Mark Zuckerberg, as a result of changes Facebook has implemented, "apps like Kogan's could no longer ask for data about a person's friends unless their friends had also authorized the app. We also required developers to get approval from us before they could request any sensitive data from people. These actions would prevent any app like Kogan's from being able to access so much data today."[24]

67. However, Facebook has done nothing to recover the Personal Information that its third-party business partners improperly harvested before the changes to its app policies.

68. Despite having been aware of the 2014 data breach since at least 2015 and having admitted that it made mistakes and breached the trust of its users, Facebook has still not individually notified its users whose Personal Information has been improperly harvested and misused, to provide them the details of the misuse of their Personal Information as required by law.

69. The stolen Personal Information is still in the hands of Cambridge Analytica and/or other third-party entities and subject to illicit use.

> Portions of the Cambridge Analytica data on as many as 50 million Facebook users may still be out in the wild, according to a report yesterday from the UK's Channel 4 News. The news organization says it has seen a cache of data dating back to the 2014 survey results Cambridge Analytica University researcher Aleksandr Kogan collected with his app "thisisyourdigitallife." Kogan later sold that data to Cambridge Analytica, which had connections to the Trump campaign and may have used it to inform election ad targeting. The data in question here "details 136,000 individuals in the US state of Colorado, along with each person's personality and psychological profile," Channel 4 reports.

---

[23] *See* https://www.facebook.com/zuck/posts/10104712037900071 (last visited March 26, 2018).

[24] *See* https://www.facebook.com/zuck/posts/10104712037900071 (last visited March 26, 2018).

> This would appear to refute Cambridge Analytica's claims as the scandal unfolded over the last two weeks that it deleted the Facebook data back in 2015 and is not guilty of any wrongdoing.
>
> . . . . .
>
> Still, the full extent of Cambridge Analytica's actions remains murky, with the company's CEO Alexander Nix suspended and facing a "full, independent investigation" of his comments made to undercover Channel 4 journalists. Those comments detailed the firm's use of bribery, blackmail, and other unsavory techniques to compromise politicians and impact geopolitical situations on behalf of its clients.

--Nick Statt, *Cambridge Analytica Reportedly Still Hasn't Deleted Facebook User Data As Promised,* The Verge (March 29, 2018).

Further Revelations That Facebook Has Allowed "Malicious Actors" To "Scrape" the Personal Profile Information of Facebook's 2 Billion Users

70. On April 4, 2018, in a startling further revelation with far-reaching implications, Facebook revealed that for years as-yet-unidentified "malicious actors" have been using Facebook search tools to "scrape" the personal profile information of "most" of Facebook's 2 billion users. Industry experts have said that, in fact, all Facebook users would have had their data taken in this described "scraping."

> Facebook said Wednesday that "malicious actors" took advantage of search tools on its platform, making it possible for them to discover the identities and collect information on most of its 2 billion users worldwide.
>
> The revelation came amid rising acknowledgement by Facebook about its struggles to control the data it gathers on users. Among the announcements Wednesday was that Cambridge Analytica, a political consultancy hired by President Trump and other Republicans, had improperly gathered detailed Facebook information on 87 million people, of whom 71 million were Americans.
>
> But the abuse of Facebook's search tools -- now disabled -- happened far more broadly and over the course of several years, with few Facebook users likely escaping the scam, company officials acknowledged. [25]

[25] *Facebook: 'Malicious Actors' Used Its Tools To Discover Identities And Collect Data On A Massive Global Scale,* Washington Post, *at* https://www.washingtonpost.com/news/the-switch/wp/2018/04/04/facebook-said-the-personal-data-of-most-its-2-billion-users-has-been-collected-and-shared-with-outsiders/?utm_term=.275ea19a3c4a (last visited 4/4/18).

71. Taking advantage of vulnerabilities in the Facebook platform that privacy experts had warned could be used to steal data, these as-yet-unidentified hackers were able to obtain Facebook users' personal information including names, addresses and telephone numbers, correlating data and building identity kits that could potentially be used for identity theft, according to the reports:

> Names, phone numbers, email addresses and other personal information amount to critical starter kits for identity theft and other malicious online activity, experts on Internet crime say. The Facebook hack allowed bad actors to tie raw data to people's real identities and build fuller profiles of them.
>
> Privacy experts had issued warnings that the phone number and email address lookup tool left Facebook users' data exposed.[26]

72. In essence, Facebook provided hackers and identity thieves with powerful tools and a treasure trove of data. Using incomplete personal information already stolen and available on the "dark web," hackers and identity thieves have been using Facebook to correlate that information with Facebook users' information to construct complete identity profiles that can be used for identity theft and fraud:

> The scam started when malicious hackers harvested email addresses and phone numbers on the so-called "Dark Web," where criminals post information stolen from data breaches over the years. Then the hackers used automated computer programs to feed the numbers and addresses into Facebook's "search" box, allowing them to discover the full names of people affiliated with the phone numbers or addresses, along with whatever Facebook profile information they chose to make public, often including their profile photos and hometown.[27]

73. Facebook has not yet disclosed the identities of the "malicious actors," exactly what personal information was taken, or how the stolen personal information was used. Facebook said it has disabled the tools used for the data theft and has taken other measures to improve security. However, as shown by the 2011 FTC consent decree, Facebook has a history

---

[26] *Id.*

[27] *Id.*

of promising to improve protections for its users' data and not fulfilling its promises.

Plaintiff and the Class Have Suffered an Injury in Fact That Will Endanger Them For Many Years to Come, If Not Forever

74. As a result of the data theft, Plaintiff's and Class members profile and Personal Information is now in the hands of Cambridge Analytica, Kogan, and other unknown parties, and Plaintiff and the Classes now face an imminent heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct. Accordingly, Plaintiff and the Class have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C.Cir. 2017).

75. Experts say that that the stolen Personal Information has likely already "spread to other groups, databases and the dark Web," making it difficult or impossible to recover the data and protect it from further misuse. "Paul-Olivier Dehaye, a privacy expert and co-founder of PersonalData.IO, said he suspects the data has already proliferated far beyond Cambridge's reach. 'It is the whole nature of this ecosystem,' Dehaye said. 'This data travels. And once it has spread, there is no way to get it back.'"[28]

76. Theft of personal information is a serious and growing problem in the United States. The 2017 Identity Fraud Report by Javelin Strategy & Research reports that, "2016 will be remembered as a banner year for fraudsters as numerous measures of identity fraud reached new heights." According to Javelin, the overall identity fraud incidence rose 16% to affect 6.15% of U.S. consumers—the highest on record--with 15.4 million U.S. identity theft victims, who lost a total of $16 billion.

77. Identity theft is a growth industry. As tracked by the Consumer Sentinel Network, maintained by the Federal Trade Commission, of the 3.1 million consumer fraud complaints filed with law enforcement and private agencies in 2015, 16 percent related to identity theft, with identity theft complaints increasing by more than 47 per cent from 2014.

78. According to a Javelin study, there is a high correlation between having

[28] *Why Facebook Users' Data Obtained By Cambridge Analytica Has Probably Spun Far Out Of Reach,* The Washington Post, Mar. 22, 2018, *at* https://www.washingtonpost.com/news/the-switch/wp/2018/03/22/why-facebook-users-data-obtained-by-cambridge-analytica-has-likely-spun-far-out-of-reach/?utm_term=.b9a50e4da142 (last visited 4/4/18).

information taken in a data breach and becoming an identity theft victim, with nearly 1 in 4 data breach letter recipients becoming an actual victim of identity fraud.

79. Identity theft victims must spend countless hours and money repairing the impact to their good name and credit record. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, tax fraud, and bank/finance fraud.

80. It can be expensive for consumers to rectify identify theft. A recent report sponsored by Experian states that the "average total cost to resolve an identity theft-related incident … came to about $20,000." Forty percent of consumers said they were never able fully to resolve their identity theft.

81. Identity theft crimes often involve more than financial loss, causing harm such as loss of reputation, adverse credit reports, and even criminal records. Identity thieves can use the victim's identity to obtain a driver's license or other licenses; commit fraud and other crimes exposing the victim to arrest; and create adverse employment, house rental and other history for the victim.

82. It is also a crime that has effects far beyond the date of the theft. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the GAO Report: "stolen data may be held for up to one year or more before being used to commit identity theft."

83. Identity theft criminals can easily sell or trade the stolen personal information on the cyber black-market. There are web sites where the stolen information is marketed surprisingly freely, according to industry sources. [29] There are also more clandestine web sites, unlisted by search engines and based in foreign countries, and on the so-called "dark web," where blocks of stolen identity information are traded or sold to anonymous buyers. Often the transactions are in bitcoin or utilize other untraceable methods of payment.

84. Plaintiff and the Classes have also been "injured in fact" in that their valuable personal, private information was misappropriated, used and sold for profit by the Defendants in

[29] *See* http://www.stopthehacker.com/2010/03/03/the-underground-credit-card-blackmarket/ (last visited April 2, 2018).

an illicit enterprise to propagandize and influence the election process, which is a concrete and particularized injury traceable to Defendants' conduct. Defendants misappropriated and misused the personal and private information for their own personal gain without the consent of, or any remuneration to, Plaintiff and the Classes.

85. Finally, Plaintiff and the Classes have been "injured in fact" in that they have been subjected to unwanted political advertising, targeted specifically to them and designed to mislead them in the free and unfettered exercise of their constitutionally protected right to vote, which is a concrete and particularized injury traceable to Defendants' conduct.

86. For all of the above reasons, Plaintiff and the Classes have suffered harm; and there is a substantial risk of additional injury to Plaintiff and members of the Classes that is imminent and concrete and that will continue for years to come.

CLASS ACTION ALLEGATIONS

87. Plaintiff brings this action on behalf of herself and two classes of Facebook users: a 2014 Data Breach Class and a Scraping Class (together "Classes").[30]

88. The 2014 Data Breach Class is initially defined as follows:

"All Facebook users in the United States whose Facebook profile information was acquired by Cambridge Analytica in June-August 2014."

Excluded from the 2014 Data Breach Class are Defendants, their corporate parents, subsidiaries, officers, directors, employees, and partners.

89. The Scraping Class is initially defined as follows:

"All Facebook users in the United States whose personal or profile information was taken by third parties using Facebook search tools."

Excluded from the Scraping Class are Defendants, their corporate parents, subsidiaries, officers, directors, employees, and partners.

90. Plaintiff reserves the right to seek to amend these class definitions or to define classes and subclasses as required, based on the investigation and research of her counsel.

91. This action has been properly brought and may properly be maintained as a class

[30] If not otherwise clear from the context, "Class" not preceded by "2014 Data Breach" or "Scraping" means and includes both Classes.

action under Rule 23(a)(1-4), Rule 23(b)(1), (2) or (3), and/or Rule 23(c)(4) of the Federal Rules of Civil Procedure and case law thereunder.

Numerosity of the Classes

(Fed. R. Civ. P. 23(a)(1))

92. Members of each Class are so numerous that their individual joinder is impractical. The Classes comprise many millions of people. The precise number of the members of each Class, and their addresses, are unknown to Plaintiff at this time, but can be ascertained from Defendants' records. Members of the Classes may be notified of the pendency of this action by mail or email, supplemented (if deemed necessary or appropriate by the Court) by published notice, including notice published on Facebook.

Predominance of Common Questions of Fact and Law

(Fed. R. Civ. P. 23(a)(2); 23(b)(3))

93. Common questions of law and fact exist as to all members of the Classes. These questions predominate over the questions affecting only individual members of the Classes. The common legal and factual questions include, without limitation:

(a) Whether Facebook represented that its users' profile and personal information in its custody was secure when in fact it was not;

(b) Whether Facebook failed to disclose that profile and personal information entrusted to it was at risk of being improperly "scraped," harvested and/or misused owing to Facebook's inadequate security procedures or reckless policies;

(c) Whether, Facebook failed to maintain reasonable procedures designed to limit the furnishing of its users' profile and Personal Information to other entities;

(d) Whether Facebook failed to implement and maintain reasonable security measures and procedures, appropriate to the information in its custody, to safeguard Class members' personal information, in violation of California Civil Code section 1798.81.5(b);

(e) Whether Defendants misappropriated Class members' data.

(f) Whether Defendants were negligent in the access, handling and protection of Class members' personal information;

(g) Whether Facebook negligently failed to warn members of the Classes of dangers with respect to the sharing of or third-party access to their profile and personal data.

(h) When Facebook became aware of the 2014 Data Breach;

(i) When Facebook became aware of the "scraping" of user data using Facebook search tools;

(j) Whether Defendants notified Class members of the taking of their data by other entities without unreasonable delay as required by California Civil Code section 1798.82;

(k) Whether Defendants' practices, actions and omissions constitute unlawful, fraudulent and/or unfair business practices in violation of California Business and Professions Code section 17200 *et seq.*;

(l) Whether Defendants were negligent with respect to the safekeeping of the profile and Personal Information in their possession;

(m) Whether Defendants are liable for unjust enrichment; and

(n) The nature of the relief, including damages and equitable relief, to which Plaintiff and members of the Classes are entitled.

Typicality of Claims

(Fed. R. Civ. P. 23(a)(3))

94. Plaintiff's claims are typical of the claims of the Classes because Plaintiff, like all other Class members, had her Personal Information in Defendant Facebook's custody exposed in the security breach.

Adequacy of Representation

(Fed. R. Civ. P. 23(a)(4))

95. Plaintiff is an adequate representative of the Classes, because her interests do not conflict with the interests of the members of the Classes and she has retained counsel competent and experienced in complex class action and consumer litigation.

96. The interests of the members of the Classes will be fairly and adequately protected by Plaintiff and her counsel.

Superiority of a Class Action

(Fed. R. Civ. P. 23(b)(3))

97. A class action is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and members of the Classes. The damages suffered by each individual members of the Classes, while significant, are small given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendant's conduct. Further, it would be virtually impossible for the members of the Classes individually to redress effectively the wrongs done to them. And, even if members of the Classes themselves could afford such individual litigation; the court system could not, given the thousands or even millions of cases that would need to be filed. Individualized litigation would also present a potential for inconsistent or contradictory judgments. Individualized litigation would increase the delay and expense to all parties and the court system, given the complex legal and factual issues involved. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief

(Fed. R. Civ. P. 23(b)(1) And (2))

98. In the alternative, this action may properly be maintained as a class action with respect to each Class, because:

(a) the prosecution of separate actions by individual members of the Classes would create a risk of inconsistent or varying adjudication with respect to individual Class members, which would establish incompatible standards of conduct for the Defendants; or

(b) the prosecution of separate actions by individual Class members would create a risk of adjudications with respect to individual members of the Classes which would, as a practical matter, be dispositive of the interests of other members of the Classes not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

99. (c) Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby making appropriate final injunctive or corresponding declaratory relief with

respect to each Class as a whole.

Issue Certification

(Fed. R. Civ. P. 23(c)(4))

100. In the alternative, common questions of fact and law, including those set forth in Paragraph 93 above, are appropriate for issue certification.

FIRST CAUSE OF ACTION

(Violation of the Stored Communication Act, 18 U.S.C § 2701, *et seq.*

(Against Facebook and Cambridge Analytica)

101. Plaintiff realleges, as if fully set forth, each and every allegation set forth above.

102. Defendant Facebook is an electronic communication provider within the meaning of the Stored Communication Act, 18 U.S.C § 2701, *et seq.* ("SCA").

103. By their actions complained of herein, Defendants have violated the SCA.

104. Defendants and each of them have violated the SCA by, among other things, intentionally accessing without authorization a facility through which an electronic communication service was provided, and/or intentionally exceeding an authorization to access that facility; and thereby obtained access to electronic communication while it was in electronic storage in such system.

105. Defendants and each of them exceeded any authorization to use Plaintiff's and Class members' stored electronic communications by allowing third parties to have access to Plaintiff's and Class members' stored electronic communications, including their profile and Personal Information.

106. Plaintiff and Class members have been damaged by Defendants' violations of the SCA.

107. Accordingly, Plaintiff and Class members are entitled to relief including compensatory and statutory damages, punitive damages, preliminary and injunctive relief, and attorneys' fees and costs, as prayed for hereunder.

SECOND CAUSE OF ACTION

(Violation of the Electronic Communications Privacy Act, 18 U.S.C §§ 2511 *et seq.*)

(Against Facebook and Cambridge Analytica)

108. Plaintiff realleges, as if fully set forth, each and every allegation set forth above.

109. By their actions complained of herein, Defendants have violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* ("ECPA").

110. The ECPA protects electronically transmitted and stored communications and data and has as its purposes safeguarding "the privacy expectations of citizens."

111. Plaintiff and Class members used Facebook to communicate and share information with friends, family, and colleagues through posts, writings, images and other intelligence, and through their Personal Information, which is electronic communications and protected by the ECPA, which protects "any transfer of signs, signals, writing, images, sound, data, or intelligence of any nature . . . " 18 U.S.C. § 2510(12).

112. Defendants and each of them violated the ECPA by, among other things, intentionally intercepting or acquiring and/or procuring other persons to intercept or acquire electronic information and communication belonging to and between Plaintiff and members of the Classes, in violation of 18 U.S.C. § Section 2511(1)(a).

113. Defendants violated the ECPA by, among other things, intentionally disclosing to other persons the contents of electronic communication, knowing or having reason to know that the information was obtained through the interception of electronic communication in violation of 18 U.S.C. § 2511(1)(c), and/or intentionally disclosing to other persons the contents of electronic communication knowing or having reason to know that the information was obtained through the interception of electronic communication in violation of 18 U.S.C. § 2511(1)(d).

114. Defendants and each of them had no lawful justification for their actions, and Plaintiff and Class members did not consent to Defendants' actions complained of herein.

115. Accordingly, Plaintiff and Class members are entitled to relief including compensatory and statutory damages, punitive damages, preliminary and injunctive relief, and attorneys' fees and costs, as prayed for hereunder.

THIRD CAUSE OF ACTION

(Violation of the Security Breach Notification Law, Cal. Civil Code § 1798.82)

(Against Facebook)

116. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein.

117. Facebook's acts and omissions violate the Security Breach Notification Law, Cal. Civil Code § 1798.82 et *seq.*

118. Facebook conducts business in California and owns or licenses digital data including, within the meaning of Cal. Civ. Code § 1798.82(h), the Personal Information of California residents, including Plaintiff.

119. Facebook's information security systems were breached, resulting in the unauthorized use of Plaintiff's and Class members' profile and Personal Information; yet, Facebook has failed to timely and properly disclose the data breach to Plaintiff and Class members.

120. Facebook learned of the 2014 Data Breach in or around 2015, and perhaps earlier, but has failed to send Plaintiff and individual Class members timely written notice as required by Cal. Civ. Code § 1798.82, and has failed to provide the information required by law.

121. By failing to timely disclose to Plaintiff and each member of the Class in the most expedient manner possible that their profile and Personal Information has been acquired by an unauthorized person, Facebook violated Cal. Civ. Code § 1798.82.

122. There was no lawful reason for the delay in notifying Plaintiff and Class members of the data breach and providing the information required by Cal. Civ. Code § 1798.82.

123. As a direct and proximate result of Facebook's violations of Cal. Civ. Code § 1798.82, Plaintiff and Class members have suffered harm and damages.

124. Plaintiff and members of the Classes are therefore entitled to damages, injunctive relief, and attorneys' fees and costs as prayed for hereunder.

FOURTH CAUSE OF ACTION

(Violation of the Customer Records Act, Cal. Civ. Code § 1798.80)

(Against Facebook)

125. Plaintiff incorporates by reference and realleges all paragraphs previously alleged herein.

126. Facebook's acts and omissions violate the California Customer Records Act, Cal. Civ. Code § 1798.80 et *seq.*

127. Facebook is a business that owns or licenses personal information about California residents within the meaning of Cal. Civ. Code § 1798.81.5.

128. By failing to implement and maintain appropriate and reasonable security procedures and practices to protect the profile and Personal Information of Plaintiff and the Classes from unauthorized access and disclosure, Facebook violated Cal. Civ. Code § 1798.81.5.

129. As a result of Facebook's violation of Cal. Civ. Code § 1798.81.5, Plaintiff and Class members have been injured.

130. Plaintiff and members of the Classes are therefore entitled to damages, injunctive relief, and reasonable attorneys' fees and costs pursuant to § 1798.84, as prayed for hereunder.

FIFTH CAUSE OF ACTION

(For Negligence and Negligent Failure to Warn)

(Against Facebook)

131. Plaintiff realleges, as if fully set forth herein, each and every allegation set forth above.

132. The actions of Defendant constitute negligence and/or negligent failure to warn.

133. Defendant owed a duty of care to Plaintiff and members of the Classes to exercise reasonable care in obtaining and protecting their profile and Personal Information, and keeping it from being compromised, misused, lost, stolen, and/or disclosed to unauthorized parties. Defendant breached that duty by failing to take appropriate and adequate security measures to protect and secure Plaintiff's and the Classes' profile and Personal Information.

134. When Plaintiff and members of the Classes registered for Facebook's services and provided their profile and Personal Information, they had the reasonable belief that Facebook

would take appropriate and adequate measures to secure and protect their information, and would warn them of dangers and inform them of any breaches or other security concerns that might call for action by them. In violation of that duty, Facebook failed to warn them of dangers inherent in its network and/or the default configuration of its system and/or their accounts and failed to prevent third parties including hackers, third parties and Cambridge Analytica from improperly obtaining Plaintiff's and the Classes' profile and Personal Information.

135. Among other things, Facebook failed to warn Plaintiff and members of the Classes that their profile and Personal Information entrusted to Facebook was not properly protected and that Facebook did not maintain the security procedures and measures reasonable necessary to protect such data from unauthorized access and use by hackers and third parties.

136. Among other things, Facebook failed to implement and maintain the security procedures, measures and protocols reasonable necessary to protect Plaintiff's and Class members' profile and Personal Information from unauthorized access and use by hackers, third parties and Cambridge Analytica.

137. Among other things, Facebook maintained known security vulnerabilities in its system, including APIs and search tools, which could be used by hackers and third party entities to "harvest" the personal information of users.

138. Among other things, Facebook failed to notify Plaintiff and members of the Classes in a timely manner that their profile and Personal Information had been taken by third parties and of the danger to them caused by the data breach and misappropriation of their profile and Personal Information.

139. As a direct and proximate result of the practices, acts and omissions alleged herein, Plaintiff and members of the Classes have suffered injury and damages.

140. At all relevant times, Plaintiff and members of the Classes acted lawfully and with due care and did not contribute to the injuries suffered.

141. Plaintiff and members of the Classes are entitled to damages and other relief, as prayed for hereunder.

SIXTH CAUSE OF ACTION

(Violations of the Unfair Competition Law, Bus. & Prof. Code §§ 17200, *et seq.*)

(Against Facebook and Cambridge Analytica)

142. Plaintiff realleges, as if fully set forth herein, each and every allegation set forth above.

143. Defendants' business practices as complained of herein violate the Unfair Competition Law, Cal. Bus. & Prof. Code sections 17200, *et seq.* ("UCL").

144. Defendants' practices constitute "unlawful" business practices in violation of the UCL because, among other things, they violate statutory law and the common law, including without limitation the Stored Communication Act, 18 U.S.C § 2701, *et seq.*, the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, the Security Breach Notification Law, Cal. Civil Code § 1798.82 et *seq.* (Facebook), and the California Customer Records Act, Cal. Civ. Code § 1798.80 et *seq.* (Facebook).

145. Defendants' actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, they are immoral, unethical, oppressive, unconscionable, unscrupulous or substantially injurious to consumers, and/or any utility of such practices is outweighed by the harm caused consumers.

146. Defendants' actions and practices constitute "fraudulent" business practices in violation of the UCL because, among other things, they have a capacity and tendency to deceive members of the public.

147. As a result of Defendants' wrongful business practices, Plaintiff and members of the Classes have suffered injury in fact.

148. Defendants' wrongful business practices present an ongoing and continuing threat to the general public.

149. Accordingly, Plaintiff and members of the Classes are entitled to relief, as prayed for hereunder.

SEVENTH CAUSE OF ACTION

(Misappropriation of Valuable Property Without Compensation)

(Against Facebook and Cambridge)

150. Plaintiff realleges, as if fully set forth herein, each and every allegation set forth above.

151. Defendants' actions constitute misappropriation.

152. Defendants and each of them used Plaintiff's and Class members' valuable personal and private information in violation of Facebook's promises to protect their privacy.

153. Plaintiff and Class members did not consent to this use.

154. Defendants and each of them gained a commercial benefit by using Plaintiff's and Class members' valuable personal and private information when Defendants misappropriated, used, and/or sold for profit Plaintiff's and Class members' valuable personal and private information.

155. Plaintiff and members of the Classes were harmed.

156. Defendants' conduct and the conduct of each of them was a substantial factor in causing Plaintiff's and Class members' harm.

157. Accordingly, Plaintiff and members of the Classes are entitled to relief, as prayed for hereunder.

EIGHTH CAUSE OF ACTION

(Unjust Enrichment)

(Against Facebook and Cambridge)

158. Plaintiff realleges, as if fully set forth, each and every allegation set forth above.

159. Plaintiff and Class members conferred a benefit upon Defendants.

160. Plaintiff and members of the Class had their profile and Personal Information, which had commercial value, stored on Facebook's network.

161. Defendants and each of them realized monetary benefit from the profile and Personal Information.

162. Defendants retained that benefit under circumstances that make it inequitable for them to retain such benefit. Specifically, Defendants retained that benefit for themselves without the consent of, or any remuneration to, Plaintiff and members of the Classes.

163. Plaintiff and members of the Classes are therefore entitled to relief, including disgorgement and/or restitution, as prayed for hereunder.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Classes pray for relief and judgment against Defendants, as follows:

A. Certifying the Classes pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Classes and designating her counsel as counsel for the Classes;

B. Awarding Plaintiff and the Classes compensatory damages, in an amount exceeding $5,000,000, to be determined by proof;

C. Awarding Plaintiff and the Classes statutory damages;

D. Awarding Plaintiff and the Classes punitive damages;

E. For preliminary relief to protect the profiles and Personal Information of Plaintiffs and members of the Classes against further misuse;

F. For declaratory and equitable relief, including restitution and disgorgement;

G. For an order enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;

H. For injunctive relief, including without limitation requiring Defendants to take steps to repair the injury caused by their wrongful conduct;

I. Awarding Plaintiff and the Classes the costs of prosecuting this action, including expert witness fees;

J. Awarding Plaintiff and the Classes reasonable attorney fees;

K. Awarding pre-judgment and post-judgment interest; and

L. Granting such other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff Christina Labajo hereby demands trial by jury of all claims so triable.

Respectfully submitted,

Date: April 5, 2018

By: /s/ Gordon M. Fauth, Jr.

Gordon M. Fauth, Jr.
Of Counsel
Rosanne L. Mah
Of Counsel
FINKELSTEIN THOMPSON LLP
100 Pine Street, Suite 1250
San Francisco, California 94111
Direct Telephone: (510) 238-9610
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Attorneys for Individual and Representative Plaintiff Christina Labajo

EXHIBIT B

U.S. District Court
California Northern District (San Francisco)
CIVIL DOCKET FOR CASE #: 3:18-cv-02090-SK

Picha v. Facebook Inc. et al
Assigned to: Magistrate Judge Sallie Kim
Demand: $500,000,000,000
Cause: 28:1332 Diversity-Tort/Non-Motor Vehicle

Date Filed: 04/05/2018
Jury Demand: Plaintiff
Nature of Suit: 370 Other Fraud
Jurisdiction: Diversity

Plaintiff

Taylor Picha

represented by **William Allan Lemkul**
Morris, Sullivan Lemkul
9915 Mira Mesa Blvd.
Suite 300
San Diego, CA 92131-2443
858-566-7600
Fax: 858-566-6602
Email: lemkul@morrissullivanlaw.com
ATTORNEY TO BE NOTICED

V.

Defendant

Facebook Inc.

Defendant

Cambridge Analytica

Date Filed	#	Docket Text
04/05/2018	1	COMPLAINT against Cambridge Analytica, Facebook Inc. (Filing fee $ 400, receipt number 0971-12251212.). Filed byTaylor Picha. (Attachments: # 1 Civil Cover Sheet)(Lemkul, William) (Filed on 4/5/2018) (Entered: 04/05/2018)
04/06/2018	2	Case assigned to Magistrate Judge Sallie Kim. Counsel for plaintiff or the removing party is responsible for serving the Complaint or Notice of Removal, Summons and the assigned judge's standing orders and all other new case documents upon the opposing parties. For information, visit *E-Filing A New Civil Case* at http://cand.uscourts.gov/ecf/caseopening. Standing orders can be downloaded from the court's web page at www.cand.uscourts.gov/judges. Upon receipt, the summons will be issued and returned electronically. Counsel is required to send chambers a copy of the initiating documents pursuant to L.R. 5-1(e)(7). A scheduling order will be sent by Notice of Electronic Filing (NEF) within two business days.

		Consent/Declination due by 4/20/2018. (srnS, COURT STAFF) (Filed on 4/6/2018) (Entered: 04/06/2018)
04/06/2018	3	Proposed Summons. (Lemkul, William) (Filed on 4/6/2018) (Entered: 04/06/2018)

PACER Service Center			
Transaction Receipt			
04/06/2018 12:18:04			
PACER Login:	gd0021DA:2553423:4036719	**Client Code:**	30993-00083
Description:	Docket Report	**Search Criteria:**	3:18-cv-02090-SK
Billable Pages:	1	**Cost:**	0.10

Will Lemkul, Esq. (CA State Bar No. 219061)
Shawn D. Morris, Esq. (CA State Bar No. 134855)
MORRIS SULLIVAN & LEMKUL LLP
9915 Mira Mesa Boulevard, Suite 300
San Diego, CA 92131
Telephone: (858) 566-7600
Facsimile: (858) 566-6602
Email: lemkul@morrissullivanlaw.com

Jodi Westbrook Flowers, *pro hac vice forthcoming*
Ann Ritter, *pro hac vice forthcoming*
Fred Baker, *pro hac vice forthcoming*
Kimberly Barone Baden (207731)
Andrew Arnold, *pro hac vice forthcoming*
Annie Kouba, *pro hac vice forthcoming*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: kbaden@motleyrice.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

Taylor Picha, individually and on behalf of all others similarly situated;

Plaintiffs,

v.

Facebook, Inc., and Cambridge Analytica,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I. INTRODUCTION

1. In a keynote speech in San Francisco in 2014, Mark Zuckerberg, CEO of Facebook, vowed, "In every single thing we do, we always put people first;" promising that Facebook would give people control over how they share their information.[1] Zuckerberg continued:

> "And in the past, when one of your friend blogged into an app [sic]... the app could ask him not only to share his data but also data that his friends had shared with him – like photos and friend list here. So now we're going to change this and we're going to make it so that now everyone has to choose to share their own data with an app themselves. So we think that this is a really important step for giving people power and control over how they share their data with the apps. And as developers, this is going to allow you to keep building apps with all the same great social features while also giving people power and control first."[2]

2. Just four years later, on March 21, 2018, Zuckerberg addressed fresh reports of the misappropriation of personal data of 50 million Facebook users by an app made by Global Science Research Ltd. and Cambridge Analytica, admitting: "This was clearly a mistake. We have a basic responsibility to protect people's data, and if we can't do that then we don't deserve to have the opportunity to serve people."[3] Then, on April 4, 2018, Facebook publicly stated that up to ***87 million users*** may have been improperly shared with Cambridge Analytica.[4] He added that he regrets the company waited so long to inform its users of what happened: "I think we got that wrong."[5]

3. This class action lawsuit is about the "wrong" Zuckerberg has admitted.

4. On March 17, 2018 *The Guardian* and *The New York Times* revealed that data

---

[1] https://singjupost.com/facebooks-ceo-mark-zuckerberg-f8-2014-keynote-full-transcript/3/?print=print.
[2] *Id.*
[3] http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html; http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-cnn-interview-transcript/index.html?iid=EL.
[4] https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM.
[5] *Id.*

analytics firm, Cambridge Analytica, harvested private information from Facebook users "on an unprecedented scale."[6] Facebook's "platform policy" at the time allowed for the accumulation of Facebook users' "friends'" data for the purpose of improved user experience, but prohibited it from being sold or used for advertising.[7]

5. Although Facebook knew about the misuse of 87 million users' data in 2015, it chose to hide this information from its users until forced to confront the issue on March 17, 2018.[8]

6. Just one month earlier, in February 2018, both Facebook and the CEO of Cambridge Analytica, Alezander Nix, told a U.K. parliamentary inquiry on fake news that the company did not have or use private Facebook data. When asked if Cambridge Analytica had Facebook user data, Simon Milner, Facebook's U.K. policy director, told U.K. officials: "They may have lots of data but it will not be Facebook user data. It may be data about people who are on Facebook that they have gathered themselves, but it is not data that we have provided."[9] Cambridge Analytica's Nix told officials: "We do not work with Facebook data and we do not have Facebook data."[10]

7. In direct contradiction to the actual events stemming from Cambridge Analytica's improper use of Facebook user data, Facebook's applicable Data Use Policy at the time of the activity stated: "Facebook does not share your information with third parties for the third parties' own and independent direct marketing purposes unless we receive your permission."[11] Facebook's current Data Use Policy states: "We do not share information that personally identifies you (personally identifiable information is information like name or email address

---

[6] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[7] *Id.*

[8] https://www.wsj.com/articles/facebook-scandal-what-to-know-about-cambridge-analytica-and-your-data-1521806400.

[9] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[10] *Id.*

[11] http://web.archive.org/web/20140103201918/https://www.facebook.com/full_data_use_policy.

that can by itself be used to contact you or identifies who you are) with advertising, measurement or analytics partners unless you give us permission."[12]

8. Plaintiff and potential class representative Taylor Picha, individually and on behalf of all others similarly situated ("Plaintiffs"), by and through the undersigned counsel, alleges the following upon personal knowledge as to her own acts and upon information and belief as to all other matters.

9. Plaintiff brings this class action against defendants Facebook, Inc. (or "Facebook") and Cambridge Analytica (or "CA") (collectively "Defendants") on behalf of all persons who registered for Facebook accounts and whose Personally Identifiable Information was obtained from Facebook by CA or other entities without authorization.

10. Cambridge Analytica is a privately held company that combines data mining and data analysis with strategic communication for use in marketing and other strategies.

11. Facebook is a social networking website. Facebook is in the business of helping people communicate with their family, friends, and coworkers online. Facebook develops technologies that facilitate the sharing of information, photographs, website links, and videos. Facebook users have the ability to share and restrict information based on their own specific criteria. By the end of 2017, Facebook had more than 2.2 billion active users.

12. Facebook's mission is "to give people the power to build community and bring the world closer together. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them."[13]

13. Facebook users "create" profiles containing personal information, including their name, birthdate, hometown, address, location, interests, relationships, email address, photos, and videos, amongst other information, referred to herein as Personally Identifiable Information (or "PII").

14. Facebook captures every IP address a user uses when logging into an account, every friend or connection made with an account (even if deleted), and all user activity (such as

---

[12] https://www.facebook.com/full_data_use_policy.
[13] https://newsroom.fb.com/company-info/.

any posts, tags in photos, "likes," status changes, and connections with other Facebook account owners).

15. This case involves the absolute disregard with which Facebook has treated Plaintiff's PII. While this information was supposed to be protected, and used for only expressly disclosed and limited purposes, CA and GSR, without authorization, or by exceeding whatever limited authorization it, or its agents, had, improperly collected the PII of nearly 87 million Facebook users.[14]

16. Facebook knew improper data aggregation was occurring and failed to stop it. Plaintiff brings this suit to protect her privacy interests and those of the class.

II. THE PARTIES

17. Plaintiff Taylor Picha (or "Plaintiff") is a resident of Charleston County, South Carolina. Plaintiff has held a Facebook account since 2007. Plaintiff is an active Facebook user and has been at all relevant times. Plaintiff recalls that during the 2016 Presidential election, she frequently saw political advertising for the Trump campaign while using Facebook.

18. Defendant Facebook is incorporated in Delaware, and the company's principal place of business is in Menlo Park, California. Facebook's securities trade on the NASDAQ under the ticker symbol "FB."

19. Defendant Cambridge Analytica is a privately held company that combines data mining and data analysis with strategic communication for the electoral process.

20. Whenever this complaint refers to any act of Defendants, the reference shall mean (1) the acts of the directors, officers, employees, affiliates, or agents of Defendants who authorized such acts while actively engaged in the management, direction, or control of the affairs of Defendants, or at the direction of Defendants, and/or (2) any persons who are the parents or alter egos of Defendants, while acting within the scope of their agency, affiliation, or employment.

[14] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.

21. A contract between Cambridge Analytica and GSR describes the objective of the data harvesting as follows: "The ultimate product of the training set is creating a 'gold standard' of understanding personality from Facebook profile information." The contract promises to create a database of 2 million "matched" profiles, identifiable and tied to electoral registers, across 11 states,[15] but with room to expand much further.

III. JURISDICTION AND VENUE

22. This Court has jurisdiction pursuant to 28 U.S.C. § 1332(d), the Class Action Fairness Act, because this suit is a class action, the parties are diverse, and the amount in controversy exceeds $5 million, excluding interest and costs. The Court has supplemental jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367.

23. Venue is proper under 28 U.S.C. §1391(c) because Defendants are corporations that do business in and are subject to personal jurisdiction in this District. Venue is also proper because a substantial part of the events or omissions giving rise to the claims in this action occurred in or emanated from this District, including decisions made by Facebook to permit the information aggregation and CA's collection of the data of personally identifiable information of the class.

IV. FACTUAL ALLEGATIONS

24. On March 17, 2018, both the *New York Times* and *The Guardian* reported on Cambridge Analytica's use of PII obtained from Facebook without permission, and under the pretext of claiming to be collecting and using it for academic purposes. The reports revealed that Cambridge Analytica, a firm hired by the Trump campaign to target voters online, used the data of 87 million people obtained from Facebook without proper disclosures or permission. The reporting also found:

[15] The states are Arkansas, Colorado, Florida, Iowa, Louisiana, Nevada, New Hampshire, North Carolina, Oregon, South Carolina, and West Virginia (*See* https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm).

> [T]he firm harvested private information from the Facebook profiles of more than 50[16] million users without their permission, according to former Cambridge employees, associates and documents, making it one of the largest data leaks in the social network's history. The breach allowed the company to exploit the private social media activity of a huge swath of the American electorate, developing techniques that underpinned its work on President Trump's campaign in 2016.
>
> ***
>
> But the full scale of the data leak involving Americans has not been previously disclosed — and Facebook, until now, has not acknowledged it. Interviews with a half-dozen former employees and contractors, and a review of the firm's emails and documents, have revealed that ***Cambridge not only relied on the private Facebook data but still possesses most or all of the trove.***[17]

(Emphasis added.)

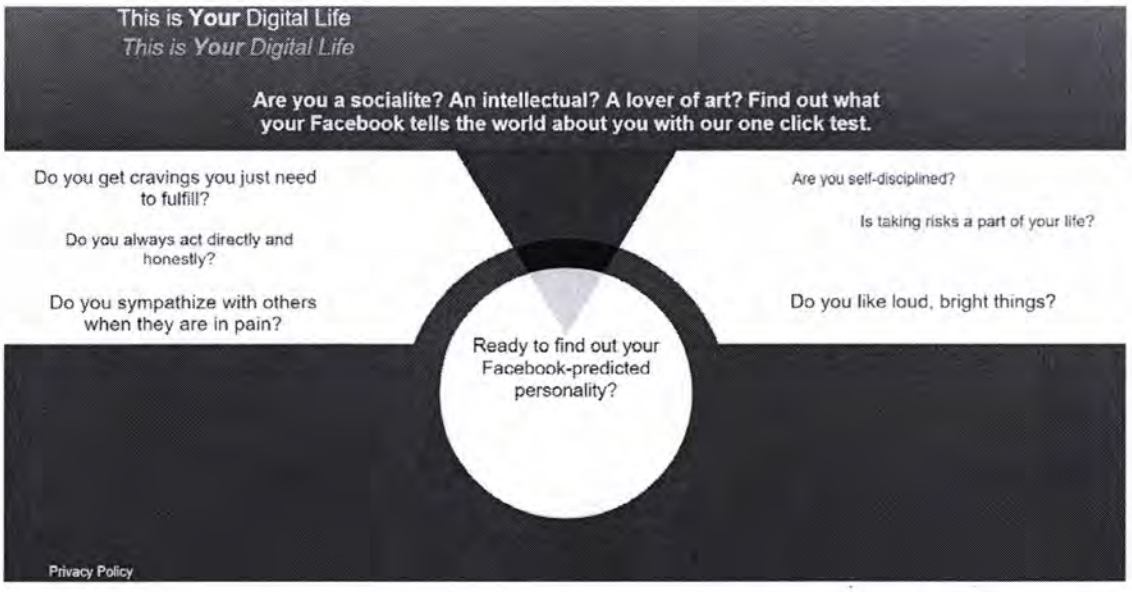
25. In 2014, Cambridge Analytica, through its parent company—Strategic Communications Laboratories (or "SCL"), hired Global Science Research Ltd. to collect Facebook user data for research purposes.[18] SCL agreed to pay GSR's data collection costs "in order to improve 'match rates' against SCL's existing datasets or to enhance GSR's algorithm's 'national capacity to profile American citizens.'"[19]

26. Global Science Research Limited (or "GSR") is a privately held company that "optimizes marketing strategies with the power of big data and psychological sciences."[20] GSR uses "innovative methods [to] produce insight on a revolutionary scale, empowering clients to understand consumers, markets, and competitors more deeply and accurately than ever before."[21] GSR was founded in 2014 by Dr. Aleksandr Kogan (or "Kogan"), a lecturer in Cambridge University's psychology department.

---

[16] Later updated to 87 million users.
[17] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
[18] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[19] *Id.*
[20] https://www.linkedin.com/company/global-science-research/.
[21] *Id.*

27. Global Science Research Ltd. collected this data by "us[ing] Amazon's crowdsourcing marketplace Mechanical Turk (MTurk) to access a large pool of Facebook profiles."[22] GSR offered users one-to-two dollars to download a survey app on Facebook called "ThisIsYourDigitalLife."[23] Billed as a "research app used by psychologists," GSR assured Facebook users that their Personally Identifiable Information would "only be used for research purposes" and remain "anonymous and safe."[24]



28. For every individual recruited on Facebook, CA and GSR not only harvested the Personally Identifiable Information of that individual, but the Personally Identifiable Information of all that individual's friends.[25] In 2014, Facebook users had an average of around 340 friends.[26]

---

[22] *Id.*
[23] https://www.ft.com/content/2034da4e-2988-11e8-b27e-cc62a39d57a0.
[24] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[25] *Id.*
[26] *Id.*

29. Approximately 270,000 people downloaded "ThisIsYourDigitalLife," giving CA and GSR a backdoor to the personal data of the original user and that of all their friends; ***more than 87 million*** other people.[27]

30. A former contractor with Cambridge Analytica, Christopher Wylie, revealed how the data mining worked: "With their profiles, likes, even private messages, [Cambridge Analytica] could build a personality profile on each person and know how best to target them with messages."[28]

31. Mr. Wylie stated that he had receipts, invoices, emails, legal letters and records that "showed how, between June and August 2014, the profiles of more than 87 million Facebook users had been harvested."[29] These profiles "contained enough information, including places of residence, that [Cambridge Analytica] could match users to other records and build psychographic profiles."[30]

32. In effect, Cambridge Analytica and Global Science Research Ltd. mounted a campaign of psychological warfare on millions of hapless victims, without their knowledge or consent. Indeed, of the 87 million Facebook users victimized by this scheme, "only about 270,000 users – those who had participated in the [thisisyourdigitallife] survey"[31]—had even consented to having their data harvested, and then only for research purposes, and without any authorization to have their data used to promote Cambridge Analytica's political goal to engage in cultural warfare. Mr. Wylie stated that ". . . Facebook data . . . was 'the saving grace' that let his team deliver the models it had promised . . . ."[32]

33. The personal information and data harvested from Facebook was used to "generate sophisticated models of each of [the Facebook users'] personalities using the so-

---

[27] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.

[28] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump.

[29] *Id.* (Facebook later reported that the number of affected users was 87 million).

[30] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[31] *Id.*

[32] *Id.*

called 'big five' personality traits and characteristics – openness, conscientiousness, extraversion, agreeableness, neuroticism (known as the OCEAN scale)."[33]

34. None of those 87 million people whose data was harvested – beyond the 270,000 who downloaded the thisisyourdigitallife app, at absolute most – consented to have their data obtained or to have their "psychographic profiles" created.

35. In response to the instant, growing scandal, Facebook initially claimed that users consented to third-party apps being able to collect their data, via their friends' act of downloading the app and nothing more,[34] describing Kogan's and GSR's acquisition of data as having been done "in a legitimate way and through the proper channels that governed all developers on Facebook at that time."[35] This is incorrect, however. Nothing in Facebook's Statement of Rights and Responsibilities ("SRR") or its Privacy Policy (the documents that form the agreement between Facebook and its users) can be read to have obtained users' consent to *any* of Kogan's and GSR's practices. The applicable portions of the SRR are as follows:

> **2. Sharing Your Content and Information**
>
> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
>
> …
>
> When you use an application, the application may ask for your permission to access your content and information as well as content and information that others have shared with you. We require applications to respect your privacy, and your agreement with that application will control how the application can use, store, and transfer that content and information. (To learn more about Platform, including how you can control what information other people may share with applications, read our Data Use Policy and Platform Page.)

[33] https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[34] *See* https://www.nytimes.com/2018/03/19 /technology/facebook-cambridge-analytica-explained.html.

[35] *See* https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

36. Indeed, the SRR affirmatively *obligates* parties using the platform to respect the privacy rights of users:

> **5. Protecting Other People's Rights**
>
> We respect other people's rights, and expect you to do the same.
>
> …
>
> *If you collect information from users, you will: obtain their consent, make it clear you (and not Facebook) are the one collecting their information, and post a privacy policy explaining what information you collect and how you will use it.*

37. While Facebook's Privacy Policy *does* address the phenomenon of third-party apps being able to acquire user information via that user's friends, Facebook's statement on the matter is patently misleading and describes a scenario entirely different from what Facebook now claims users consented to:

> **Controlling what is shared when the people you share with use applications**
>
> *…If an application asks permission from someone else to access your information, the application will be allowed to use that information only in connection with the person that gave the permission, and no one else.*
>
> For example, some apps use information such as your friends list, to personalize your experience or show you which of your friends use that particular app.

(italics and underline added)

38. These examples are far afield of the full extent of the "friends permission" functionality – including the use of that functionality that was sanctions by Facebook. Accordingly, Facebook is patently wrong when it suggests that users consented or otherwise authorized *any* of the conduct at issue.

39. The trove of data about a user's friends to developers was exceedingly detailed. The exfiltrated information appears to relate to virtually every aspect of a person's life as embodies on Facebook: their birthday, their hometown, their religious and political

affiliations, their work history, and also highly personal data such as location check-ins, and even the friends' photos and videos.[36]

Facebook's History of Privacy Failures

40. In 2007, Facebook initiated a tracking program called Beacon, which took information from approximately 87 million users' purchases and activities on other websites and posted it to their News Feed, without clearly asking for the user's approval.

41. Weeks after Beacon's introduction, Facebook users responded by signing a petition to drop the feature, citing concerns over privacy. In response, Facebook created an "opt out" from the service. Zuckerberg commented, "[w]e simply did a bad job with this release, and I apologize."[37] In March 2010, Facebook settled a class action for $9.5 million to resolve claims regarding its Beacon feature.

42. In 2008, Facebook introduced "Open ID," which allowed users to log in to other websites with their Facebook credentials. Facebook also made its "like" button available on other websites, further blurring the lines of privacy and allowing for widespread tracking of a person's web browsing history—even non-Facebook users.[38]

43. One year after the initial launch of "Open ID," Facebook changed its default settings to make users' profiles public by default. Users objected to this move, but it took Facebook five years to change the default to be visible to users' friends only.[39]

44. In December 2009, Facebook changed its website so that certain information that users may have designated as private was made public. Facebook didn't warn users of this change or get their prior approval. Facebook represented that third-party apps installed by users would have access only to user information needed to operate, when in fact, the apps (and their developers) could access nearly all of users' Personal Identifiable

---

[36] *See* http://www.businessinsider.com/what-data-did-cambridge-analytica-have-access-to-from-facebook-2018-3.

[37] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.

[38] *Id.*

[39] *Id.*

Information – data the apps didn't need. Facebook users were told they could limit the sharing of their personal data to "Friends Only;" however, selecting "Friends Only" did not prevent users' Personal Identifiable Information from being shared with third-party applications their friends used. Facebook also promised it would not share users' personal data with advertisers; however, it did.

45. Upon receiving a number of complaints, the Federal Trade Commission (or "FTC") investigated Facebook's privacy practices in 2011 which resulted in a consent decree barring Facebook from making any further deceptive privacy claims, required Facebook to obtain consumers' approval before it changed the way it shared users' personal data, and required Facebook to obtain periodic assessments of its privacy practices by independent, third-party auditors for 20 years.[40] In response to the consent decree, Facebook's Zuckeberg stated, "I'm the first to admit that we've made a bunch of mistakes … [w]e can also always do better. I'm committed to making Facebook the leader in transparency and control around privacy."[41]

46. Facebook, Inc. was forewarned of the possible consequences of its privacy practices through its international subsidiary.

47. In August 2011, Facebook user Max Schrems, a German privacy rights lawyer, filed a complaint against Facebook Ireland (Defendant Facebook's Irish subsidiary and the location of its European headquarters) with the Irish-based Office of the Data Protection Commissioner (or "ODPC") concerning the access and use of Facebook users' personal data by developers of third-party applications which "constitute[d] a tremendous threat to data privacy on facebook.com."[42] Schrems went on to state that Facebook Ireland had no way "to ensure compliance with the[] limited contractual measures" it imposed on

---

[40] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111205facebookfrn.pdf.

[41] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.

[42] https://noyb.eu/wp-content/uploads/2018/03/Media-Update-Cambridge-Analytica-en.pdf.

developers.[43] Furthermore, while Facebook supposedly requires third-party applications to have a privacy policy, not all apps have one: "[w]hen the user connects to an application that does not have a privacy policy, facebook.com simply hides the link that would usually bring you to the privacy policy, instead of warning the user that there is not even a privacy policy."[44]

48. As a result of Schrems' complaint, the ODPC investigated and issued a "Report of Re-Audit" (or "Report") on September 21, 2012, which noted that Facebook Ireland had failed to adopt complete protection of "sensitive personal data."[45] Specifically, the ODPC recommended to Facebook Ireland that:

- Users must be sufficiently empowered via appropriate information and told to make a fully informed decision when granting access to third party applications;
- It must be easier for users to understand that their activation and use of an app will be visible to their friends as a default setting;
- It should be easier for users to make informed choices about what apps installed by friends can access personal data about them.[46]

49. In June 2013, Facebook notified six million users of a data breach involving that their contact information, including phone numbers and emails. This data breach also revealed that Facebook had been merging users' information with data submitted by their contacts in order to create fuller profiles of its users. Essentially, personal data of non-Facebook users whose information may have been uploaded by friends that are Facebook users was being collected by Facebook and may have been inadvertently exposed in the breach.[47]

---

[43] *Id.*
[44] *Id.*
[45] https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf.
[46] *Id.*
[47] https://www.msn.com/en-us/money/companies/facebooks-past-failures/ar-BBKyhST?li=BBnb7Kz.

50. Cambridge Analytica was created in 2013 by its British parent company, Strategy Communications Laboratories Group Limited and Robert Mercer, reported to be a "secretive hedge fund billionaire" participating in American politics. Christopher Wylie stated the company's mission as: "[they] want to fight a culture war in America."[48] The Cambridge Analytica website discloses that it has offices in Washington, DC and in New York,[49] but upon information and belief, it is neither registered to do business nor is licensed to conduct business in either jurisdiction.

51. In 2015, Cambridge Analytica gained recognition as the data analysis company retained by the Ted Cruz presidential primary campaign, but after that campaign faltered in 2016, Cambridge Analytica worked for the Donald Trump presidential campaign.[50] An interview with CA's CEO, Alexander Nix, confirms that the Trump campaign paid for Cambridge Analytica's services and that then-candidate Trump was "a good businessman."[51]

52. During the Ted Cruz presidential campaign of 2015, Global Science Research Ltd. and Cambridge Analytica faced similar allegations of unauthorized use of PII from tens of millions of Facebook users for targeted marketing.[52] At the time, Facebook stated, "misleading people or misusing [users'] information is a direct violation of our policies and we will take swift action against companies that do, including banning those companies from Facebook and requiring them to destroy all improperly collected data."[53]

53. On September 11, 2017, the Spanish Agency for Data Protection (or "AEPD") announced that it had fined Facebook €1.2 million euros for violating data protection regulations following its investigation to determine whether the data processing carried out by the Company complied with the data protection regulations. The AEPD stated that its

---

[48] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
[49] https://cambridgeanalytica.org/.
[50] https://en.wikipedia.org/wiki/Cambridge_Analytica.
[51] https://www.forbes.com/sites/parmyolson/2018/03/20/face-to-face-with-cambridge-analytica-alexander-nix-facebook-trump/#674008da535f.
[52] *Id.*
[53] *Id.*

investigation made it possible to verify that Facebook does not inform the users in a comprehensive and clear way about the data that it collects and the treatments it carrie out with them, but that it is limited to giving some examples. In particular, the AEPD found that Facebook collects other data derived from the interaction carried out by users on the platform and on third-party sites without them being able to clearly perceive the information that Facebook collects about them or with what purpose they are going to use it. The AEPD also found that the privacy policy of Facebook contains generic and unclear expressions, and requires access to a multitude of different links to view it. Further, the AEPD concluded that Facebook makes an inaccurate reference to the way it uses the data it collects, so that Facebook users with an average knowledge of new technologies would not become aware of Facebook's data collection, storage, or use policies.[54]

54. In May 2017, the French data protection authority fined Facebook its maximum allowable fine of €150,000 for violations similar to those claimed by the Spanish authorities. "Facebook proceeded to a massive compilation of personal data of internet users in order to display targeted advertising'" complained the Commission Nationale de 'Informatique et des Libertés. "It has also been noticed that Facebook collected data on browsing activity of internet users on third-party websites without their knowledge."[55]

55. More recently, the allegations in a lawsuit filed by the makers of Pikinis, an app that was shut down three years ago when Facebook finally cut off third-party access to a back-door channel to friends' data, also undermine Facebook's suggestion that it has always placed user privacy interests at the forefront of its business. Pikinis alleged that Facebook engaged in "an anti- competitive bait-and-switch scheme" that duped Six4Three and tens of thousands of other developers into making hefty investments to build apps and then decided "it would be in Facebook's best interest to no longer compete with many developers and to shut down their businesses." While Facebook has denied any wrongdoing in the Pikinis lawsuit, its response confirms that Facebook has always had the ability to change its practices

[54] http://fortune.com/2017/09/11/facebook-privacy-fine-spain/.
[55] https://www.nytimes.com/2017/05/16/technology/facebook-privacy-france-netherlands.html.

with respect to third party developers, but did not. "Facebook made -- and must continue to make – important editorial decisions about what third party content is available through its platform to protect its users' privacy and experience," the company argued in a February 2018 court filing.[56]

56. While the plethora of earlier "red flag" warnings should have caused Facebook to seriously address what was a systemic problem with its privacy and data security practices, the so-called "White Paper" that Alex Stamos (Facebook's Chief Information Security Officer) co-authored, entitled "Information Operations and Facebook," unquestionably alerted Defendant that those activities were pervasive and supported by management. The "White Paper" also confirmed that Facebook's public statements were false and misleading. Among other things, the White Paper affirmatively misrepresented that Facebook had "no evidence of any Facebook accounts being compromised" in connection with the 2016 election as of the date it was published on April 27, 2017.

57. Stamos said that he had initially provided a written report to Facebook executives concerning the circumstances which led to the harvest of Facebook users' Personal Identifiable Information by Cambridge Analytica, but instead of taking appropriate action and disclosing the incident, the report was rewritten and presented as a hypothetical scenario; which appeared in the whitewashed "White Paper" that Facebook published to further suppress and conceal its wrongdoing.

Facebook Regarded User Privacy and Data Security as Paramount to Its Business Model, but Failed to Uphold Its Own Policies

58. Maintaining user privacy and data security has long been considered in Facebook's business and growth prospects. A June 21, 2013 blog post entitled, "Important Message from Facebook's White Hat Program" states: "At Facebook, we take people's privacy seriously, and we strive to protect people's information to the very best of our

[56] https://www.bloomberg.com/news/articles/2018-03-21/facebook-is-trying-to-protect-bikini-photos-but-it-s-not-easy.

ability. We implement many safeguards, hire the brightest engineers and train them to ensure we have only high-quality code behind the scenes or your Facebook experiences . . . ***Your trust is the most important asset we have, and we are committed to improving our safety procedures and keeping your information safe and secure.***"[57]

59. However, prior to this blog post, Facebook had experienced at least one major attack to its security systems and represented that it was "working continuously" to prevent similar security threats in the future. A February 15, 2013 post entitled, "Protecting People On Facebook" states:

> Facebook, like every significant internet service, is frequently targeted by those who want to disrupt or access our data and infrastructure. As such, ***we invest heavily in preventing, detecting, and responding to threats that target our infrastructure, and we never stop working to protect the people who use our service.*** The vast majority of the time, we are successful in preventing harm before it happens, and our security team works to quickly and effectively investigate and stop abuse.
>
> Last month, Facebook Security discovered that our systems had been targeted in a sophisticated attack. As soon as we discovered the presence of the malware, we remediated all infected machines, informed law enforcement, and began a significant investigation that continues to this day. We have found no evidence that Facebook user data was compromised.
>
> As part of our ongoing investigation, we are working continuously and closely with our own internal engineering teams, with security teams at other companies, and with law enforcement authorities to learn everything we can about the attack, and how to prevent similar incidents in the future.
>
> ***
>
> We will continue to work with law enforcement and the other organizations and entities affected by this attack. It is in everyone's interests for our industry to work together to prevent attacks such as these in the future.[58]

(Emphasis added.)

60. An October 16, 2015 post by Stamos, stated:

---

[57] https://www.facebook.com/notes/facebook-security/important-message-from-facebooks-white-hat-program/10151437074840766/.

[58] https://es-la.facebook.com/notes/facebook-security/protecting-people-on-facebook/10151249208250766/.

> ***The security of people's accounts is paramount at Facebook, which is why we constantly monitor*** for potentially malicious activity and offer many options to proactively secure your account. Starting today, we will notify you if we believe your account has been targeted or compromised by an attacker suspected of working on behalf of a nation-state.
>
> ***
>
> While we have always taken steps to secure accounts that we believe to have been compromised, we decided to show this additional warning if we have a strong suspicion that an attack could be government-sponsored. We do this because these types of attacks tend to be more advanced and dangerous than others, and we strongly encourage affected people to take the actions necessary to secure all of their online accounts.
>
> It's important to understand that this warning is not related to any compromise of Facebook's platform or systems, and that having an account compromised in this manner may indicate that your computer or mobile device has been infected with malware. Ideally, people who see this message should take care to rebuild or replace these systems if possible.
>
> To protect the integrity of our methods and processes, we often won't be able to explain how we attribute certain attacks to suspected attackers. That said, we plan to use this warning only in situations where the evidence strongly supports our conclusion. We hope that these warnings will assist those people in need of protection, and we will continue to improve our ability to prevent and detect attacks of all kinds against people on Facebook.[59]

(Emphasis added.)

61. Stamos once told his security team that he explained to upper management that Facebook has "the threat profile of a Northrop Grumman or a Raytheon or another defense contractor, but we run our corporate network, for example, like a college campus, almost."[60] Stamos repeatedly butted heads with Facebook executives over the lack of security with their platform. He once had 120 people under his direction in Facebook's security group, but as of earlier this month there are only three.[61]

62. At all relevant times, Facebook has maintained a Data Use Policy on its website. At all relevant times, the Data Use Policy advised Facebook users, in part:

---

[59] https://www.facebook.com/notes/facebook-security/notifications-for-targeted-attacks/10153092994615766/.

[60] https://www.nytimes.com/2018/03/20/technology/alex-stamos-facebook-security.html.

[61] https://www.nytimes.com/2018/03/19/technology/facebook-alex-stamos.html.

> Granting us permission to use your information not only allows us to provide Facebook as it exists today, but it also allows us to provide you with innovative features and services we develop in the future that use the information we receive about you in new ways. While you are allowing us to use the information we receive about you, you always own all of your information. ***Your trust is important to us, which is why we don't share information we receive about you with others unless we have:***
>
> - ***received your permission***
> - ***given you notice, such as by telling you about it in this policy; or***
> - ***removed your name and any other personally identifying information from it.***[62]

(Emphasis added.)

63. In a post to the Company's website on March 18, 2018, Facebook Vice President Adam Bosworth noted that maintaining user privacy is in the Company's best interests:

> Yes developers can receive data that helps them provide better experiences to people … [we] have this set up in a way so that no one's personal information is sold to businesses.
>
> ***
>
> If people aren't having a positive experience connecting with businesses and apps then it all breaks down. This is specifically what I mean when we say [Facebook's] interests are aligned with users when it comes to protecting data."[63]

64. When Kogan created his app in 2013, Facebook allowed developers to collect information on friends of those who chose to use third-party apps if their privacy settings allowed it. In an email to university colleagues, Kogan said that in 2014, after he founded GSR, he transferred the app to the company and used an official Facebook Inc. platform for developers to change the terms and conditions of his app from "research" to "commercial use," and that at no point then did the social media company object. Kogan's email further stated: "Through the app, we collected public demographic details about each user (name, location, age, gender), and their page likes (e.g., the Lady Gaga page). We collected the same data about their friends whose security settings allowed for their friends

[62] https://www.facebook.com/full_data_use_policy.
[63] https://www.wired.com/story/facebook-privacy-transparency-cambridge-analytica/.

to share their data through apps. Each user who authorized the app was presented with both a list of the exact data we would be collecting, and also a Terms of Service detailing the commercial nature of the project and the rights they gave us as far as the data. Facebook themselves have been on the record saying that the collection was through legitimate means."[64]

65. Kogan's position contradicts Facebook's stance that Kogan violated the company's terms and services and then lied about it. "We clearly stated that the users were granting us the right to use the data in broad scope, including selling and licensing the data," Kogan wrote in a March 18, 2018 email obtained by Bloomberg. "These changes were all made on the Facebook app platform and thus they had full ability to review the nature of the app and raise issues." Facebook's position is suspect given revelations regarding its relationship with Cambridge Analytica and the fact that Facebook researchers co-authored a study with Kogan in 2015 that also used data harvested by a Facebook app.[65]

66. Although Facebook claims it did not receive notice of Cambridge Analytic harvesting users' personal data until 2015, its response to an inquiry from WIRED regarding the incident confirms that Facebook personnel were aware of similar user privacy issues by at least 2014, and knew that updates to Facebook's policies and data security practices were necessary to alleviate concerns that had already expressed by Facebook users. "In 2014, after hearing feedback from the Facebook community, we made an update to ensure that each person decides what information they want to share about themselves, including their friend list," Facebook stated. "Before you decide to use an app, you can review the permissions the developer is requesting and choose which information to share. You can manage or revoke those permissions at any time."[66]

67. Even after Facebook changed its policy in 2014 supposedly to protect user information from being exploited by "bad actors," Facebook gave developers a ***full year***

[64] https://www.bloomberg.com/news/articles/2018-03-21/facebook-app-developer-kogan-defends-his-actions-with-user-data.
[65] *Id.*
[66] https://newsroom.fb.com/news/2018/03/suspending-cambridge-analytica/.

before it ended their access to friends' newsfeeds and photos. Worse, Facebook failed to follow up on suspicious activity when security protocols were triggered, as noted by Wylie.

68. Facebook's failure to detect and prevent the harvesting of Personal Identifiable Information by Cambridge Analytica, or to adequately respond with proper notification and disclosures to Facebook users in accordance with best practices and applicable laws, belies any claim that Facebook's actual "monitoring" practices and internal data security and privacy policies were sufficient. Facebook's user privacy data security practices were woefully inadequate.

69. The incident has violated the privacy of millions of people in every State. The privacy and personal, sensitive information of 87 million people is now at high risk for identity theft and compromise, and will continue to be at risk as a direct result of the acts of Defendants.

Government Investigations and Lawsuits

70. In the days after the breach was publicly revealed, the Attorneys General of New York and Massachusetts announced an investigation into Facebook and Cambridge Analytica.[67] On March 19, 2018, Senator Ron Wyden followed up with a detailed series of questions for Facebook to answer.[68]

71. Senators Amy Klobuchar, Democrat of Minnesota, and John Kennedy, Republican of Louisiana, have asked the chairman of the Judiciary Committee, Charles E. Grassley, Republican of Iowa, to hold a hearing.[69] Republican leaders of the Senate Commerce Committee, organized by John Thune of South Dakota, wrote a letter to Mr. Zuckerberg demanding answers to questions about how the data had been collected and if users were able to control the misuse of data by third parties.[70] "It's time for Mr.

---

[67] https://ag.ny.gov/press-release/statement-ag-schneiderman-facebookcambridge-analytica.
[68] https://www.wyden.senate.gov/imo/media/doc/wyden-cambridge-analytica-to-facebook.pdf.
[69] https://www.marketwatch.com/story/sens-klobuchar-kennedy-call-for-hearing-on-facebook-google-twitter-2018-03-19.
[70] https://www.commerce.senate.gov/public/_cache/files/6499b47b-05e8-49fc-90c2-6ff56dd9bf65/8D44CEC37FF5FC2C421C71962F62D998.facebook-letter-03.19.2018.pdf.

Zuckerberg and the other C.E.O.s to testify before Congress," Senator Mark Warner, Democrat of Virginia, said on Tuesday. "The American people deserve answers about social media manipulation in the 2016 election."[71]

72. On March 20, 2018, a committee in the British Parliament sent a letter to Defendant Zuckerberg and asked him to appear before the panel to answer questions on the company's connection to Cambridge Analytica. The president of the European Parliament also requested an appearance by Mr. Zuckerberg. "The committee has repeatedly asked Facebook about how companies acquire and hold on to user data from their site, and in particular about whether data had been taken without their consent," wrote Damian Collins, chairman of the British committee. "***Your officials' answers have consistently understated this risk, and have been misleading to the committee.***"[72]

73. On March 21, 2018, a former Facebook employee told British lawmakers that his concerns about lax data protection policies at the Company went ignored by "senior executives." Sandy Parakilas, who worked as a platform operations manager from 2011 to 2012, appeared before the U.K. parliament committee investigating the impact of social media on recent elections. "I made a map of the various data vulnerabilities of the Facebook platform," Parakilas told the committee. "I included lists of bad actors and potential bad actors," he said, "and said here's some of the things these people could be doing and here's what's at risk."[73] When asked by the committee if any of those executives were still at the company, Parakilas said they were, but declined to name them in public. Parakilas previously told *The Guardian* on March 20, 2018 that he had warned senior executives at Facebook about how the Company's data protection policies posed a risk of breach. Parakilas explained, "My concerns were that all of the data that left Facebook servers to developers could not be monitored by Facebook."[74] He also said that Facebook

---

[71] https://twitter.com/MarkWarner/status/976067286732869632.

[72] http://www.bbc.com/news/uk-43474760.

[73] https://www.bloomberg.com/news/articles/2018-03-21/facebook-ex-employee-tells-u-k-lawmakers-data-warnings-ignored.

[74] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

could have prevented the collection of Personal Identifiable Information by Cambridge Analytica.

74. Parakilas was initially told that any decision to ban an app required the personal approval of the chief executive, Mark Zuckerberg.

75. From 2007 until mid-2014, Facebook allowed developers to access the personal data of friends of people who used apps by the "friends permission" functionality. This allowed tens of thousands of developers to access user data without the consent of those users.

76. Facebook had two incentives to offer up user data for these purposes. First, developers created third party content that was then hosted on Facebook and enticed users to return often. In addition, Facebook took a 30% cut of any payments made to those developers' apps.

77. Parakilas believes that "a majority of Facebook users" have had their data exfiltrated, without their consent, by unknown third parties. The use of the data continues to this day, with no oversight and in direct violation of the most basic autonomy and privacy rights of the individuals who have been – and continue to be – profiled.[75]

78. Parakilas, stated that as many as "[h]undreds of millions of Facebook users are likely to have had their private information harvested by companies that exploited the same terms as the firm that collected data and passed it on to Cambridge Analytica."[76]

79. Incredibly, Facebook's "trust model" was rife with security vulnerabilities and a near total abnegation of its responsibility to audit its own rules limiting use of Facebook data by third parties. Or, in Parakilas' own words, "[Facebook] felt that it was better not to know."[77]

---

[75] *Id.*

[76] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas.

[77] *Id.*

80. That company philosophy and practice has continued since Mr. Parakilas' departure from Facebook, as evidenced by the improper harvesting and hijacking of more than 87 million of the company's user profiles by Cambridge Analytica. Facebook's stated position—that "Protecting people's information is at the heart of everything we do"[78]—is in direct contradiction with the truth: That fact, Facebook knew about this security breach for two years, but did little or nothing to protect its users.[79]

81. On March 19, 2018, *Bloomberg* reported "FTC Probing Facebook For Use of Personal Data, Source Says," disclosing that the U.S. Federal Trade Commission (or "FTC") is "probing whether Facebook violated terms of a 2011 consent decree of its handling of user data that was transferred to Cambridge Analytica without [user] knowledge."[80] Under a 2011 settlement with the FTC, Facebook "agreed to get user consent for certain changes to privacy settings as part of a settlement of federal charges that it deceived consumers and forced them to share more personal information than they intended."[81]

82. The current FTC investigation involves similar concerns about Facebook's user privacy practices. In an interview with *The New York Times,* David Vladeck, former director of the FTC's Bureau of Consumer Protection, said the Cambridge Analytica incident may have violated Facebook's 2011 consent decree. "There are all sorts of obligations under the consent decree that may not have been honored here," he said.[82] In another interview, with *The Washington Post*, Vladeck stated, "I will not be surprised if at

---

[78] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[79] *Id.*; https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge-analytica-sandy-parakilas

[80] https://www.bloomberg.com/news/articles/2018-03-20/ftc-said-to-be-probing-facebook-for-use-of-personal-data

[81] https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; https://www.ftc.gov/sites/default/files/documents/cases/2011/12/111205facebookfrn.pdf

[82] https://www.nytimes.com/2018/03/20/business/ftc-facebook-privacy-investigation.html.

some point the FTC looks at this. I would expect them to[.]"[83] Jessica Rich, who also served as director of the bureau and was deputy director under Vladeck, said, "Depending on how all the facts shake out, Facebook's actions could violate any of all of these provision, to the tune of many millions of dollars in penalties. They could also constitute violations of both U.S. and EU laws," adding, "Facebook can look forward to multiple investigations and potentially a whole lot of liability here."[84]

83. "We are aware of the issues that have been raised but cannot comment on whether we are investigating," an FTC spokeswoman said in a statement on March 20, 2018. "We take any allegations of violations of our consent decrees very seriously."[85]

84. Concerning the FTC investigation into the potential violations of the 2011 consent decree, Facebook's deputy chief privacy officer, Rob Sherman, stated: "We remain strongly committed to protecting people's information … We appreciate the opportunity to answer questions the FTC may have."[86] If Facebook violated terms of the consent decree, it could face fines of more than $40,000 a day per violation.

V. CLASS ACTION ALLEGATIONS

85. Plaintiff bring this class action claim pursuant to Rule 23 of the Federal Rules of Civil Procedure. The requirements of Rule 23 are met with respect to the class defined below.

86. Plaintiff brings her claims on her own behalf, and on behalf of the following class (the "Class"):

> All persons who registered for a Facebook account in the United States whose Personally Identifiable Information was obtained from Facebook by Cambridge Analytica, or other entities, without authorization or in excess of authorization.

---

[83] https://www.washingtonpost.com/business/economy/us-and-european-officials-question-facebooks-protection-of-personal-data/2018/03/18/562b5b0e-2ae2-11e8-911f-ca7f68bff0fc_story.html?utm_term=.78754f22e61b.

[84] *Id.*

[85] http://money.cnn.com/2018/03/20/technology/ftc-pressure-facebook/.

[86] *Id.*

87. Excluded from the Class are Defendants and any entities in which any Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants' officers, agents, and employees. Also excluded from the Class are the judge assigned to this action, and any member of the judge's immediate family.

88. Plaintiff reserves the right to amend or modify the Class definition in connection with a motion for class certification and/or the result of discovery. This lawsuit is properly brought as a class action for the following reasons.

89. The Class is so numerous that joinder of the individual members of the proposed Class is impracticable. Plaintiff reasonably believes that the Class includes eighty-seven (87) million people or more in the aggregate and well over 1,000 in the smallest of the classes. The precise number and identities of Class members are unknown to Plaintiff, but are known to Defendants and can be ascertained through discovery regarding the information kept by Defendants or their agents.

90. Questions of law or fact common to the Class exist as to Plaintiff and all Class members, and these common questions predominate over any questions affecting only individual members of the Class. The predominant common questions of law and/or fact include the following:

a. Whether Facebook represented that it would safeguard Plaintiff's and Class members' Personally Identifiable Information and not to disclose it without consent;

b. Whether Cambridge Analytica improperly obtained Plaintiff's and Class members' Personally Identifiable Information without authorization or in excess of any authorization;

c. Whether Facebook was aware of the improper collection of Plaintiff's and Class members' Personally Identifiable Information by Cambridge Analytica;

d. Whether Facebook owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

e. Whether Facebook breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personally Identifiable Information;

f. Whether Class members' Personally Identifiable Information was obtained by CA and/or other unauthorized third-parties;

g. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

h. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

i. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;

j. Whether Facebook breached its promises of privacy to its users;

k. Whether Plaintiff and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and

l. Whether Plaintiff and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

91. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiff and the Class. Individual questions, if any, pale by comparison to the numerous common questions that predominate.

92. Plaintiff's claims are typical of the claims of Class members. The injuries sustained by Plaintiff and the Class flow, in each instance, from a common nucleus of operative facts based on the Defendants' uniform conduct as set forth above. The defenses, if any, that will be asserted against Plaintiff's claims likely will be similar to the defenses that will be asserted, if any, against Class members' claims.

93. Plaintiff will fairly and adequately protect the interests of Class members. Plaintiff has no interests materially adverse to or that irreconcilably conflict with the

interests of Class members and have retained counsel with significant experience in handling class actions and other complex litigation, and who will vigorously prosecute this action.

94. A class action is superior to other available methods for the fair and efficient group-wide adjudication of this controversy, and individual joinder of all Class members is impracticable, if not impossible. The cost to the court system of individualized litigation would be substantial. Individualized litigation would likewise present the potential for inconsistent or contradictory judgments and would result in significant delay and expense to all parties and multiple courts hearing virtually identical lawsuits. By contrast, a class action presents fewer management difficulties, conserves the resources of the parties and the courts and protects the rights of each Class member.

95. Defendants have acted on grounds generally applicable to the entire Class, thereby making injunctive relief or corresponding declaratory relief appropriate with respect to the Class as a whole.

96. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether (and when) Facebook knew about the improper collection of Personally Identifiable Information;

b. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

c. Whether Facebook's representations that they would secure and not disclose without consent the Personally Identifiable Information of Plaintiff and members of the classes were facts that reasonable persons could be expected to rely upon when deciding whether to use Facebook's services;

d. Whether Facebook misrepresented the safety of its many systems and

services, specifically the security thereof, and its ability to safely store Plaintiff's and Class members' Personally Identifiable Information;

e. Whether Facebook failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

f. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

g. Whether Defendants' conduct violated Cal. Bus. & Prof. Code § 22575, *et seq.*;

h. Whether Facebook breached its promises of privacy to its users;

i. Whether Defendants failed to adhere to their posted privacy policy concerning the care they would take to safeguard Plaintiff's and Class members' Personally Identifiable Information in violation of California Business and Professions Code § 22576;

i. Whether Defendants negligently and materially failed to adhere to their posted privacy policy with respect to the extent of their disclosure of users' data, in violation of California Business and Professions Code § 22576;

COUNT ONE

Negligence as Against Facebook

97. Plaintiff hereby incorporates all the above allegations by reference as if fully set forth herein. Plaintiff asserts this count individually and on behalf of the proposed Class.

98. Defendants owed a duty to Plaintiff and the Class to exercise reasonable care in obtaining and protecting their Personally Identifiable Information, and keeping it from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.

99. Defendants knew that the Personally Identifiable Information of Plaintiff and the Class was personal and sensitive information that is valuable.

100. By being entrusted by Plaintiff and the Class to safeguard their Personally Identifiable Information, Facebook had a special relationship with Plaintiff and the Class. Plaintiff and the Class signed up for Facebook's services and agreed to provide their Personally Identifiable Information with the understanding that Facebook would take appropriate measures to protect it, and would inform Plaintiff and the Class of any breaches or other security concerns that might call for action by Plaintiff and the Class. But, Facebook did not. Facebook failed to prevent Cambridge Analytica and Global Science Research Ltd. from improperly obtaining Plaintiff's and the Class Members' Personally Identifiable Information.

101. Defendants breached their duties by failing to adopt, implement, and maintain adequate security measures to safeguard the Personally Identifiable Information, or by obtaining that Personally Identifiable Information without authorization.

102. Facebook breached its duties by allowing a third-party to access and obtain the Personally Identifiable Information of approximately 87 million users that did not consent to provide this information to either Facebook or Cambridge Analytica.

103. Facebook further breached its duties by failing to confirm that Cambridge Analytica had deleted users' Personally Identifiable Information after it became aware of the breach of information.

104. Facebook also breached their duty to timely disclose that Plaintiff's and the other class members' Personally Identifiable Information had been, or was reasonably believed to have been, improperly obtained. Facebook first discovered that its users' information had been improperly obtained in at least 2015, but did not disclose the privacy breach until media pressure forced it to respond on March 22, 2018.

105. Cambridge Analytica had a duty to refrain from obtaining Plaintiff's and the Class Members' Personally Identifiable Information without their consent or authorization.

106. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiff and the Class, their Personally Identifiable Information would not have been

improperly obtained. Defendants' negligence was a direct and legal cause of the theft of the Personally Identifiable Information of Plaintiff and the Class and all resulting damages.

107. The injury and harm suffered by Plaintiff and the Class members was the reasonably foreseeable result of Defendants' failure to exercise reasonable care in safeguarding and protecting Plaintiff's and the other class members' Personally Identifiable Information.

108. These damages include, but are not limited to, invasion of privacy, theft of PII, increased risk of data breaches, increased risk of identity theft, emotional distress, lost time, effort and money in responding to Facebook's negligence and misuse of their personal data beyond what Facebook promised.

COUNT TWO

Violations of the Stored Communications Act, 18 U.S.C. § 2701, *et seq*.

109. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

110. Facebook is an electronic communications provider within the meaning of the Stored Communications Act ("SCA").

111. Under the Stored Communications Act, an entity providing an electronic communication service to the public "shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service." 18 U.S.C. § 2702(a)(1).

112. The servers Facebook uses to provide its electronic communications service to Facebook users are a "facility" within the meaning of the SCA.

113. Facebook and Cambridge Analytica are "persons" within the meaning of the SCA.

114. Section 2701(a)(1) of the Stored Communications Act authorizes a private right of action for damages, injunctive relief and equitable relief against any person who "intentionally exceeds an authorization to access (a facility through which an electronic

communication service is provided] … and thereby obtains … access to wire or electronic communication while it is in electronic storage in such system…"

115. Facebook intentionally exceeded any authorization they may have had to Plaintiff's and other users' stored electronic communications by allowing Global Science Research Limited and Cambridge Analytica to have access to Plaintiff's and other users' stored electronic communications which also contained sensitive personal information.

116. Facebook knowingly allowed Global Science Research Limited and Cambridge Analytica and as yet unknown other possible third parties to intentionally exceed any authorization it may have had to Plaintiff's and other users' stored electronic communications.

117. Facebook's provision of 'users' personal data to third parties and Cambridge Analytica's acquisition of the same as alleged herein exceeded any authorization from any party to the personal data at issue.

118. Because of the architecture of Facebook's servers, the sharing of personal data among Facebook users results in and constitutes interstate data transmissions.

119. Plaintiff and Class members have been harmed by Defendants' misconduct and are entitled to statutory damages, actual damages and reasonable attorneys' fees and costs, as well as declaratory and injunctive relief.

COUNT THREE

Violations of California's Unfair Competition Law ("UCL") – Unlawful Business Practices (Cal. Bus. & Prof. Code § 17200, *et seq.*)

120. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

121. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

122. Facebook represented that it would not disclose user's Personally Identifiable Information without consent and/or notice. It also required application

developers, like Cambridge Analytica and Global Science Research Ltd., to obtain and utilize users' Personally Identifiable Information in specified, limited ways.

123. Facebook failed to abide by these representations. Facebook did not prevent improper disclosure of Plaintiff's and the Class Members' Personally Identifiable Information.

124. Facebook stored the Personally Identifiable Information of Plaintiff and members of the Class in its electronic and consumer information databases. Defendants represented to Plaintiff and members of the classes that their Personally Identifiable Information would remain private. Defendants engaged in unfair acts and business practices by representing that they would not disclose this Personally Identifiable Information without authorization, and/or by obtaining that Personally Identifiable Information without authorization.

125. Cambridge Analytica obtained Plaintiff's and the Class Members' Personally Identifiable Information either wholly without authorization or in excess of any authorization it—or its agents—may have obtained.

126. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a), and Cal. Bus. & Prof. Code § 22576 (as a result of Facebook failing to comply with its own posted policies).

127. In Silicon Valley, data is currency. Plaintiff and the Class members suffered injury in fact and lost money or property as the result of Defendants' unlawful business practices. In particular, Plaintiff and Class members Personally Identifiable Information was "harvested" and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the information at issue in this case is of tangible value.

128. In particular, Plaintiff and Class members Personally Identifiable Information was taken and is in the hands of those who will use it for their own advantage, or is being sold for value, making it clear that the hacked information is of tangible value.

129. As a result of Defendants' unlawful business practices and violation of the UCL, Plaintiff and the class are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief.

COUNT FOUR

Violations of the California Invasion of Privacy Act (Cal. Penal Code §§ 630, *et seq.*)

130. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

131. Plaintiff, individually and on behalf of Class Members, asserts violations of the CIPA, Cal. Penal Code § §630, *et seq.*, specifically Cal. Penal Code §§ 631(a), 632, and 637.7(d) for Cambridge Analytica's unlawful interception and use the contents of Facebook users' personal and private communications and for the unlawful acquisition of Plaintiffs and Class members' location data, without consent.

132. Cambridge Analytica used and/or continues to use this information for the purposes of profiling, marketing, and advertising.

133. Facebook was aware that Cambridge Analytica used and/or uses its users' personal and private communications in this inappropriate manner, and took no action to protect or even notify its uses. Additionally, Facebook provided the platform and lack of privacy protections that made Cambridge Analytica's misconduct possible. Facebook profited from Cambridge Analytica's misconduct.

134. Cal. Penal Code § 630 provides that "The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society."

135. Defendants' acts in violation of the CIPA occurred in the State of California because those acts resulted from business decisions, practices, and operating policies that

Facebook developed, implemented, and utilized in the State of California and which are unlawful and constitute criminal conduct in the state of Facebook's residence and principal business operations. Facebook's implementation of its business decisions, practices, and standard ongoing policies that violate the CIPA took place and continue to take place in the State of California. Defendants profited and continue to profit in the State of California as a result of its repeated and systemic violations of the CIPA. Defendants' unlawful conduct, which occurred in the State of California, harmed and continues to harm Plaintiff and Class Members.

136. Plaintiff and Class Members sent and received private messages, private wall posts, status updates, and other private communications via Facebook's services.

137. Defendants are not, and were not at any time, a party of Plaintiff's and Class Members' private messages.

138. The private messages, status updates, wall posts, and other private communications exchanged among Plaintiff and Class Members are messages.

139. These messages are communications among Plaintiff and Class Members.

A. Violations of Cal. Penal Code § 631(a)

140. Pursuant to Cal. Penal Code § 7, Defendants, corporations, are "persons."

141. Defendants use a "machine," "instrument," "contrivance," or "in any other manner" are able to, read or to learn the content or meaning of Plaintiff's and Class Members' private messages.

142. Defendants act willfully when they read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private messages.

143. Defendants do not have the consent of any party to the communication, or they act in an unauthorized manner, when they read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private messages.

144. Plaintiff's and Class Members' private Facebook communications are "any message, report, or communication."

145. At the time Defendants read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private communications, the private communications are in transit.

146. At the time Defendants read, attempt to read, or learn the content or meaning of Plaintiff's and Class Members' private communications, the private communications are passing over any wire, line, or cable.

147. Private Facebook communications – coded, written messages sent electronically to remote locations – are telegraphs within the meaning of the CIPA and this section of CIPA. As such, the wires, lines, cables, and/or instruments which carry and facilitate the transmission of Plaintiff's and Class Members private Facebook communications are telegraph wires, lines, cables and/or instruments within the meaning of the CIPA and CIPA § 631(a).

148. Plaintiff and Class Members do not consent, expressly or impliedly, to Defendants' eavesdropping upon and recording of their private communications. Defendants do not disclose material information to Facebook users relating to their attempts at, among other things, intercepting, storing, and analyzing the contents of users' private communications.

149. There is no knowledge or expectation among Plaintiff and Class Members regarding the extent of Defendants' reading of private communications, learning about the content or meaning of such content, the acquisition of such content, the collection of such content, or the manipulation of such content for pecuniary gain. Each and every one of these actions extends beyond the normal occurrences, requirements, and expectations regarding the facilitation and transmission of Facebook's private communication.

B. Violations of Cal. Penal Code § 632

150. Pursuant to Cal. Penal Code §§ 7 and 632(b), Defendants, corporations, are "persons."

151. Cal. Penal Code § 632 prohibits eavesdropping upon or the recording of any confidential communication, including those occurring by telephone, telegraph, or other device, through the use of an amplification or electronic recording device without the consent of all parties to the communication.

152. Defendants intentionally and without the consent of any party to the communications, eavesdrops upon and/or records and uses the contents of Plaintiff's and Class Members' private communications.

153. Defendants use electronic amplifying or recording devices, including Cambridge Analytica's data gathering technology, to eavesdrop upon and to record Plaintiff's and Class Members' private communications, for purposes independent and unrelated to storage.

154. Plaintiff's and Class Member's private communications are confidential communications with specifically identified and designated recipients.

155. At the time Plaintiff and Class Member transmit private messages, status updates, wall posts, or other private communications through Facebook, their communications are confidential because the communications are confined to those persons specified as recipients in the destination address fields as pertaining to private messages, and are confined to pre-determined "friends" as to other communications on a private profile. There neither would nor could be any expectation that a third party, such as Cambridge Analytica or Facebook, would act in any manner other than to facilitate the communication of the private message between the sender and the intended recipient or recipients. There certainly would not and could not be any expectation that Cambridge Analytica – through Facebook – would be able to access a trove of personal information and private communications without the consent or knowledge of Plaintiff or Class Members with the intent to use such information for profiling, political advertising, and other non-academic and commercial purposes.

156. There is no knowledge or expectation among Plaintiff and Class Members regarding the extent of Defendants' reading and use of users' private communications

content, learning about the content or meaning of those private communications, acquiring and collecting the content of such communications, and manipulating the content of such communications – each action being beyond the normal occurrences, requirements, and expectations regarding the facilitation and transmission of private communications on Facebook.

157. Plaintiff's and Class Members' private communications sent via Facebook are carried on among the parties by means of an electronic device that is not a radio.

158. Plaintiff and Class Members do not consent, expressly or impliedly, to Defendants' eavesdropping upon and recording of their private communications. Neither Facebook nor Cambridge Analytica disclosed material information to Facebook users relating to their attempts to read, scan, acquire, collect, and manipulate the contents of users' private communications.

159. While Plaintiff has identified certain accused devices and/or technology in this Complaint, Plaintiff reserves the right to assert violations of Cal. Penal Code §§ 631 and 632 as to any further devices or technology subsequently discovered or any devices or technology upon which Facebook provides additional information.

C. Violations of Cal. Penal Code § 637.7

160. As defined under CIPA, "'electronic tracking device' means any device attached to a vehicle *or other movable thing that reveals its location or movement by the transmission of electronic signals*." § 637.7(d). CIPA expressly prohibits the use of "an electronic tracking device to determine the location or movement of a person." Cal. Pen. Code § 637.7(a).

161. Among the data points harvested by Facebook and provided to the remaining Defendants (as well as all third-party developers who used the "friends permission" feature) was the location of Plaintiff's and Class Members.

162. Facebook acquired – and Cambridge Analytica exfiltrated and used – Plaintiff's and Class Members' location through, *inter alia*, location data associated with smartphones and other mobile devices running Facebook.

163. Plaintiffs and Class members did not consent to said acquisition of location information by any Defendant.

D. Relief Sought Under Cal. Penal Code § 637.2

164. As a result of Defendants' violations of Cal. Penal Code §§ 631, 632, and 637, Plaintiff and the Class are entitled to:

a. Preliminary and permanent injunctive relief to require Facebook and Cambridge Analytica to fully disclose the extent of their activities, to seek the informed and knowing consent of all Facebook users when gathering private communications data, and to halt their violations;

b. Appropriate declaratory relief;

c. Monetary relief in the amount set forth in Cal. Penal Code § 637.2(a) for each Class Member; and

d. Reasonable attorney's fees and other litigation costs reasonably incurred.

COUNT FIVE

Invasion of Privacy – Intrusion Upon Seclusion

165. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

166. Plaintiff and Class Members have reasonable expectations of privacy in their online behavior on Facebook.

167. The reasonableness of such expectations of privacy is supported by Facebook's unique position to monitor Plaintiff's and Class Members' behavior through its access to Plaintiff's and Class members' user data. It is further supported by the surreptitious, highly-technical, and non-intuitive nature of Defendants' collective tracking and exfiltrating of

Plaintiff's and Class Members' personal data, via third party apps that Class members did not download, much less provide authorization for such behavior.

168. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs. Facebook intentionally designed its platform – and established commensurate policies and procedures governing such platform – to enable the exfiltration, without authorization, of Class Members' personal data by third-party apps such as "thisisyourdigitallife." Defendants intentionally availed themselves of Facebook's privacy-invasive measures in order to acquire Class Members' personal data without consent.

169. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs by intentionally facilitating the exfiltration of Class Members' personal data to surreptitiously obtain, improperly gain knowledge of, review, and/or retain Plaintiff's and Class members' personal data and activities through the monitoring technologies and policies described herein.

170. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices – not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiff's and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

171. Plaintiff and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

172. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

173. As a result of Defendants' actions, Plaintiff and Class Members seek injunctive relief, in the form of (1) destruction of all data obtained by Cambridge Analytica; (2)

certification by Facebook that no third parties presently are able to access Plaintiff's and Class Members' user data without first obtaining express consent; (3) audits, by Facebook, of all third parties who obtained user data through the "friends permissions" feature; (4) notification, by Facebook to Plaintiff and Class members, of each instance in which a third party obtained user data – including the type of user data – via the "friends permissions" feature; and (5) destruction of all improperly obtained user data of Plaintiff and Class Members.

174. As a result of Defendants' actions, Plaintiff and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiff and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiff and made in conscious disregard of Plaintiff's rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT SIX

Violation of the California Constitution Article I, Section I

175. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

176. Plaintiff and Class Members have reasonable expectations of privacy in their online behavior on Facebook.

177. The reasonableness of such expectations of privacy is supported by Facebook's unique position to monitor Plaintiff's and Class Members' behavior through its access to Plaintiff's and Class Members' user data. It is further supported by the surreptitious, highly technical, and non-intuitive nature of Defendants' collective tracking and exfiltrating of Class Members' personal data, via third party apps that Class Members did not download, much less provide authorization for such behavior.

178. Defendants intentionally intruded on and into Plaintiff's and Class Members' solitude, seclusion, or private affairs. Facebook intentionally designed its platform – and established commensurate policies and procedures governing such platform – to enable the exfiltration, without authorization, of Class Members' personal data by third-party apps such as

"thisisyourdigitallife." Defendants intentionally availed themselves of Facebook's privacy-invasive measures in order to acquire Class Members' personal data without consent.

179. These intrusions are highly offensive to a reasonable person. This is evidenced by, *inter alia*, the immense outcry following the revelation of these acts and practices – not only from the public, but also from regulators and legislators. Further, the extent of the intrusion cannot be fully known, as the nature of privacy invasion involves sharing Plaintiff's and Class Members' personal information with potentially countless third-parties, known and unknown, for undisclosed and potentially unknowable purposes, in perpetuity. Also supporting the highly offensive nature of Defendants' conduct is the fact that Defendants' principal goal was to surreptitiously monitor Plaintiff's and Class Members—in one of the most private spaces available to an individual in modern life—and to allow third-parties to do the same.

180. Plaintiff and Class Members were harmed by the intrusion into their private affairs as detailed throughout this Complaint.

181. Defendants' actions and conduct complained of herein were a substantial factor in causing the harm suffered by Plaintiff and Class Members.

182. As a result of Defendants' actions, Plaintiff and Class Members seek injunctive relief, in the form of (1) destruction of all data obtained by Cambridge Analytica; (2) certification by Facebook that no third parties presently are able to access Plaintiffs' and Class members' user data without first obtaining express consent; (3) audits, by Facebook, of all third parties who obtained user data through the "friends permissions" feature; (4) notification, by Facebook to Plaintiffs and Class members, of each instance in which a third party obtained user data – including the type of user data – via the "friends permissions" feature; and (5) destruction of all improperly obtained user data of Plaintiffs and Class members.

183. As a result of Defendants' actions, Plaintiffs and Class members seek nominal and punitive damages in an amount to be determined at trial. Plaintiffs and Class members seek punitive damages because Defendants' actions – which were malicious, oppressive, willful – were calculated to injure Plaintiffs and made in conscious disregard of Plaintiffs' rights. Punitive damages are warranted to deter Defendants from engaging in future misconduct.

COUNT SEVEN

Declaratory Relief Pursuant to 28 U.S.C. § 2201

184. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

185. An actual controversy, over which this Court has jurisdiction, has arisen and now exists between the parties relating to the legal rights and duties of Plaintiff and Defendants for which Plaintiff desires a declaration of rights.

186. Plaintiff contends and Defendants dispute that Defendants, in whole or in part, were authorized by Plaintiff and Class Members to acquire user data via the "friends permissions" functionality without the express consent, from each developer, of all users whose personal data was thereby acquired.

187. Plaintiff, on behalf of himself and the Class is entitled to a declaration that Defendants were *not* so authorized through their contracts with Facebook, and accordingly that Defendants' behavior violated the Stored Communications Act, CIPA, the UCL, and Plaintiff's common law claims.

COUNT EIGHT

Conversion

188. Plaintiff incorporates all of the above allegations by reference as if fully set forth herein.

189. Plaintiff and Class Members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiff's and Class Members' rights to possess and control such property, to which they had a superior right of possession and control at the time of conversion.

190. As a direct and proximate result of Defendants' conduct, Plaintiff and the Class Members suffered injury, damage, loss or harm and therefore seek compensatory damages.

191. In converting Plaintiff's Private Information, Defendants have acted with malice, oppression and in conscious disregard of the Plaintiff and Class Members' rights. Plaintiff, therefore, seeks an award of punitive damages on behalf of the class.

VI. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the other Class members, respectfully requests that this Court enter a judgment against Defendants as follows:

(a) Certifying the Nationwide Class and appointing Plaintiff as Class Representative;

(b) Finding that Defendants' conduct was negligent, deceptive, unfair, and unlawful as alleged herein;

(c) Enjoining Defendants from engaging in further negligent, deceptive, unfair, and unlawful business practices alleged herein;

(d) Awarding Plaintiff and the Class members nominal, actual, compensatory, and consequential damages;

(e) Awarding Plaintiff and the Class members statutory damages and penalties, as allowed by law;

(f) Awarding Plaintiff and the Class members restitution and disgorgement;

(g) Awarding Plaintiff and the Class members pre-judgment and post-judgment interest;

(h) Awarding Plaintiff and the Class members reasonable attorneys' fees costs and expenses, and;

(i) Granting such other relief as the Court deems just and proper.

VII. DEMAND FOR JURY TRIAL

Plaintiff, individually and on behalf of all others similarly situated, demands a trial by jury on all issues so triable.

DATED: April 5, 2018

Respectfully Submitted,

/s/ Will Lemkul
Will Lemkul (State Bar No. 219061)
MORRIS SULLIVAN & LEMKUL LLP
9915 Mira Mesa Boulevard
Suite 300
San Diego, CA 92131
Telephone: (858) 566-7600
Facsimile: (858) 566-6602
Email: lemkul@morrissullivanlaw.com

/s/ Jodi Westbrook Flowers
Jodi Westbrook Flowers, *pro hac vice forthcoming*
Ann Ritter, *pro hac vice forthcoming*
Fred Baker, *pro hac vice forthcoming*
Kimberly Barone Baden (207731)
Andrew Arnold, *pro hac vice forthcoming*
Annie Kouba, *pro hac vice forthcoming*
MOTLEY RICE LLC
28 Bridgeside Boulevard
Mount Pleasant, SC 29464
Telephone: (843) 216-9000
Facsimile: (843) 216-9450
Email: jflowers@motleyrice.com
Email: aritter@motleyrice.com
Email: fbaker@motleyrice.com
Email: kbaden@motleyrice.com
Email: aarnold@motleyrice.com
Email: akouba@motleyrice.com

Attorneys for Plaintiff and the proposed class